

NETGEAR®

Manuel d'utilisation principal

Entièrement switchs manageables série M4350

Micrologiciel version 14.0.0 et versions ultérieures

Septembre 2025
202-12813-02

NETGEAR, Inc.

Support et communauté

Visitez <https://www.netgear.com/fr/support/> pour obtenir des réponses à vos questions et accéder aux derniers téléchargements.

Vous pouvez également consulter notre communauté NETGEAR sur community.netgear.com pour obtenir des conseils sur votre produit.

Réglementation et aspects juridiques

Si ce produit est vendu au Canada, vous pouvez accéder à ce document en français canadien à <https://www.netgear.com/fr/support/download/>.

(Si ce produit est vendu au Canada, vous pouvez accéder à ce document en français canadien à l'adresse <https://www.netgear.com/fr/support/download/>.)

Pour les informations à propos de la conformité réglementaire, y compris la Déclaration de conformité pour l'UE, rendez-vous sur <https://www.netgear.com/fr/about/regulatory/>.

Avant de brancher l'alimentation, reportez-vous au document de conformité légale.

Pour connaître la politique de confidentialité de NETGEAR, rendez-vous sur le site <https://www.netgear.com/fr/about/privacy-policy/>.

Lorsque la loi le permet, en utilisant cet appareil, vous acceptez les conditions générales de NETGEAR sur le site <https://www.netgear.com/fr/about/terms-and-conditions> et, si vous n'acceptez pas, retournez l'appareil à votre lieu d'achat pendant votre période de retour.

Ce produit est conçu et garanti pour une utilisation en intérieur uniquement. N'utilisez pas cet appareil à l'extérieur. La source PoE est destinée à une connexion à l'intérieur d'un bâtiment uniquement.

Marques commerciales

© NETGEAR, Inc., NETGEAR et le logo NETGEAR sont des marques commerciales de NETGEAR, Inc. Toutes les marques commerciales autres que NETGEAR sont utilisées à des fins de référence uniquement.

Historique de révision

Numéro de pièce de publication	Date de publication	Commentaires
202-12813-02	Septembre 2025	EN: 202-12688-04 Nous avons ajouté les sections suivantes : • <u>Configurer un VLAN basé sur oui</u> à la page 331 et les sous-sections : ◦ <u>Ajoutez une configuration VLAN basée sur oui</u> à la page 331 ◦ <u>Supprimer une configuration VLAN basée sur oui</u> à la page 332 • <u>Activer ou désactiver le mode de profil AVB global Auto-lag</u> à la page 480 • <u>Configurez le mode de hachage global non unicast</u> à la page 483 Nous avons ajouté une remarque sur le passage du mode géré engagement au mode géré Insight dans la section suivante : • <u>Présentation de l'interface utilisateur principale et autres options de gestion</u> à la page 31 Nous avons ajouté des informations sur le Precision Time Protocol qui prend en charge la version 2,0 et les capacités de coexistence PTP BC et TC : • <u>Horloge transparente a protocole temporel de PRECISION</u> à la page 136 • <u>Horloge limite de protocole de temps de précision et horloge grand maître</u> à la page 139 • <u>Gérez les paramètres de l'horloge limite PTP globale et de l'horloge grand maître</u> à la page 140
202-12813-01	Décembre 2024	EN: 202-12688-03 Première publication.

Sommaire

Chapitre 1 Démarrez avec l'interface utilisateur principale

Publications disponibles et aide en ligne.....	30
Commutateurs pris en charge.....	30
Enregistrer votre produit.....	31
Présentation de l'interface utilisateur principale et autres options de gestion.....	31
Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web.....	33
Connectez-vous à l'interface utilisateur principale à l'aide de l'adresse IP par défaut du commutateur.....	34
Connectez-vous à l'interface utilisateur principale avec une adresse IP connue.....	35
Principaux boutons de l'interface utilisateur et champs définis par l'utilisateur.....	36
Conventions de dénomination des interfaces.....	37
Enregistrez vos paramètres dans la configuration en cours....	38
Aide en ligne de l'interface utilisateur principale.....	38
Utilisez la vue périphérique dans l'interface utilisateur principale.....	39
Configurez l'accès SNMPv3.....	41
Découvrez et intégrez le commutateur au contrôleur NETGEAR engage.....	43
Comment Insight et l'interface utilisateur principale interagissent l'un avec l'autre.....	45
Informations d'identification de l'interface utilisateur principale.	46

Chapitre 2 Gérer la superposition

Présentation de l'empilement des commutateurs.....	49
Synchronisation et mise à niveau du micrologiciel de pile.....	50
Maintenance de la configuration de la pile.....	51
Sélection du commutateur de gestion de pile.....	51
Comportement de réinitialisation par défaut de la pile.....	52
Limites d'empilement.....	52
Configurer une pile.....	53
Définissez le mode d'échantillonnage de la pile.....	54
Ajoutez un commutateur comme commutateur de gestion de pile.....	55
Ajoutez un membre de la pile ou un commutateur de gestion de secours.....	57

Modifiez le réglage d'un commutateur dans la pile.....	60
Retirez un commutateur de la pile.....	61
Configurez le mode pile pour un port.....	62
Configurer la synchronisation du micrologiciel de pile.....	65
Configurez le mode de hachage de la jonction.....	66
Affiche des informations sur la configuration de la pile.....	68
Affiche l'état de la pile de messages de pulsation.....	70
Affiche les informations de diagnostic, d'état et de chemin du port de pile.....	71
Retirez une pile.....	72
Transfert continu de pile.....	74
Configurer le transfert continu et afficher les informations associées.....	75
Afficher les statistiques de point de contrôle de transfert ininterrompu.....	77

Chapitre 3 Configurer les informations système du commutateur

Informations sur le système et le logement du commutateur....	82
Afficher et configurer les informations système du commutateur.....	82
Afficher l'état du ventilateur.....	84
Afficher les informations du capteur de température.....	86
Afficher l'état du périphérique et la version du micrologiciel.....	87
Afficher l'état de l'UC du système.....	89
Configurez les seuils de CPU.....	90
Afficher ou effacer les statistiques du commutateur.....	92
Afficher les informations sur le périphérique USB.....	94
Affiche des informations sur une pile et les modèles de commutateur optionnels pour une pile.....	96
Interfaces de bouclage.....	98
Interfaces de gestion IPv4 et VLAN.....	99
Configurez le port de service IPv4.....	100
Configurez un VLAN de gestion IPv4.....	102
Configurer une interface de gestion IPv4.....	104
Interfaces de gestion IPv6 et VLAN.....	106
Configurez un port de service IPv6.....	107
Gérer les adresses IPv6 pour le port de service IPv6.....	109
Configurez un VLAN de gestion IPv6.....	110
Gérer les adresses IPv6 pour le VLAN de gestion IPv6.....	113
Gérer les adresses de route IPv6 par défaut pour le VLAN de gestion IPv6.....	115
Configurer une interface de gestion IPv6.....	116
Gérer les adresses IPv6 pour l'interface de gestion IPv6.....	118

Gérer les adresses de route IPv6 par défaut pour l'interface de gestion IPv6.....	120
Paramètres heure et NTP.....	121
Configurez les paramètres NTP globaux.....	121
Affiche l'état NTP global et les informations sur les paquets.	124
Configurer les serveurs NTP.....	126
Ajoutez un serveur NTP.....	127
Modifiez les paramètres d'un serveur NTP existant.....	129
Supprimez un serveur NTP.....	130
Configurer les paramètres de l'heure d'été.....	131
Afficher l'état de l'heure d'été.....	134
Horloge transparente a protocole temporel de PRECISION....	136
Gérer les paramètres PTP TC globaux.....	136
Gérer les paramètres de l'interface PTP TC.....	137
Horloge limite de protocole de temps de précision et horloge grand maître.....	139
Gérez les paramètres de l'horloge limite PTP globale et de l'horloge grand maître.....	140
Gérer les paramètres de l'interface de l'horloge limite PTP.	144
Afficher ou effacer les statistiques de l'horloge limite PTP....	146
Afficher des informations détaillées sur l'horloge limite PTP.	148
Système de noms de domaine.....	151
Configurez les paramètres DNS globaux et ajoutez un serveur DNS.....	151
Supprimer un serveur DNS.....	153
Configurer et afficher les informations de nom d'hôte en adresse IP.....	155
Ajoutez une entrée statique à la table de mappage dynamique des hôtes.....	155
Supprimez une entrée de la table de mappage dynamique des hôtes.....	156
Maintenez la table de mappage dynamique des hôtes et affichez les entrées.....	157
Changer de modèle de gestion de base de données.....	158
Paramètres Ethernet verts.....	160
Configurez les paramètres Ethernet verts globaux.....	160
Configurez les paramètres de l'interface Ethernet verte.....	162
Configurer et afficher les paramètres Ethernet verts détaillés d'une interface.....	164
Affiche des informations Ethernet vertes pour le partenaire de liaison d'une interface.....	166
Affichez le résumé vert des statistiques Ethernet.....	167
Paramètres Bonjour.....	169
Activez ou désactivez Bonjour.....	170
Affiche les informations Bonjour.....	171

Activer ou désactiver la capacité du serveur TFTP.....	172
Serveur DHCP IPv4.....	173
Configurez un serveur DHCP.....	173
Ajoutez une classe DHCP à utiliser avec l'option DHCP 82...	175
Configurez une classe DHCP.....	176
Gérer les pools DHCP.....	177
Créez un pool DHCP.....	178
Modifier un pool DHCP.....	180
Supprimer un pool DHCP.....	181
Configurez les options de pool DHCP.....	182
Lier un pool DHCP à une classe et configurer la liaison.....	184
Afficher les statistiques du serveur DHCP.....	185
Afficher les liaisons DHCP.....	187
Supprimez une ou toutes les liaisons DHCP dynamiques....	188
Afficher les liaisons avec conflits DHCP.....	189
Supprimez une ou toutes les liaisons DHCP présentant des conflits.....	191
Relais DHCP.....	192
Configurez les paramètres de relais DHCP globaux et affichez les statistiques de relais.....	192
Configurez une interface de relais DHCP.....	195
Relais DHCP de couche 2.....	197
Configurez les paramètres globaux du relais DHCP L2.....	197
Configurez une interface de relais DHCP L2.....	198
Affiche les statistiques de l'interface de relais L2 DHCP.....	201
Relais UDP.....	202
Configurez les paramètres de relais UDP globaux et ajoutez un relais UDP.....	202
Modifier la configuration d'un relais UDP.....	204
Supprimer une configuration de relais UDP.....	205
Ajoutez une configuration d'interface UDP.....	206
Modifier une configuration d'interface UDP.....	208
Supprimer une interface UDP.....	209
Serveur DHCPv6.....	210
Activez le serveur DHCPv6.....	210
Gérer les pools DHCPv6.....	212
Créez un pool DHCPv6.....	212
Modifier un pool DHCPv6.....	213
Supprimer un pool DHCPv6.....	214
Gérer la délégation du préfixe DHCPv6 pour les pools.....	215
Créez une configuration de délégation de préfixe DHCPv6 pour un pool.....	215
Modifier une configuration de délégation de préfixe DHCPv6 pour un pool.....	217

Supprimez une configuration de délégation de préfixe DHCPv6 pour un pool.....	218
Configurez les paramètres cos d'une interface	219
Afficher les liaisons DHCPv6.....	221
Afficher les statistiques du serveur DHCPv6.....	223
Supprimez les statistiques DHCPv6 pour une ou toutes les interfaces.....	225
Interface de relais DHCPv6.....	227
Power over Ethernet.....	228
Concepts PoE.....	229
Définissez le seuil d'utilisation du système PoE et le mode de gestion de l'alimentation.....	232
Configurez les paramètres du port PoE.....	235
Redémarrez un ou plusieurs ports PoE.....	240
Gérer le seuil d'utilisation de PoE.....	241
Gérer la redondance de l'alimentation N+1.....	243
Affiche des informations sur la gestion de plusieurs sources d'alimentation pour l'alimentation PoE.....	245
Programmations de minuterie.....	247
Créez un programme de minuterie.....	248
Spécifiez les paramètres d'une planification de minuterie PoE absolue	249
Spécifiez les paramètres d'une planification de minuterie PoE récurrente	251
Modifiez les paramètres d'une entrée de planification de minuterie PoE récurrente	253
Supprimer une entrée de programmation de minuterie.....	255
Supprimer un planning de minuterie.....	256
Simple Network Management Protocol.....	257
Gérer les communautés SNMPv1 et SNMPv2.....	257
Ajoutez une communauté SNMPv1 et SNMPv2.....	257
Modifier une communauté SNMPv1 et SNMPv2 existante.	259
Supprimez une communauté SNMPv1 et SNMPv2.....	260
Gérez les paramètres de déROUTement SNMPv1 et SNMPv2.	261
Ajoutez une configuration d'interruption SNMPv1 ou SNMPv2 pour un hôte.....	261
Modifier une configuration d'interruption SNMPv1 ou SNMPv2 pour un hôte.....	263
Supprimez une configuration d'interruption SNMPv1 ou SNMPv2 pour un hôte.....	264
Configurer les drapeaux d'interruption SNMPv1 et SNMPv2 ..	265
Afficher les MIB prises en charge.....	270
Gérer les utilisateurs SNMPv3.....	271
Ajoutez un compte utilisateur SNMPv3.....	271
Modifier un compte utilisateur SNMPv3.....	272

Supprimer un compte utilisateur SNMPv3.....	273
LLDP (Link Layer Discovery Protocol).....	274
Configurez les paramètres LLDP globaux.....	275
Configurer les paramètres de l'interface LLDP.....	276
Afficher ou effacer les statistiques LLDP.....	278
Affiche les informations sur le périphérique local LLDP.....	280
Affiche les informations sur le périphérique distant LLDP....	282
Afficher l'inventaire des périphériques distants LLDP.....	283
Protocole de découverte de couche de liaison pour les périphériques de point d'extrémité multimédia.....	285
Configurez les paramètres globaux LLDP-MED.....	285
Configurer les paramètres de l'interface LLDP-MED.....	287
Affiche les informations sur le périphérique local LLDP-MED.	289
Affiche les informations sur le périphérique distant LLDP-MED.....	291
Afficher l'inventaire des périphériques distants LLDP-MED..	294
Dépendance de liens.....	295
Configurer un groupe de dépendances de liens.....	296
Configurer ou afficher les interfaces en amont et en aval pour un groupe de dépendances de liens.....	298
Effacer toutes les interfaces d'un groupe de dépendances de liens.....	300
Protocole de découverte standard de l'industrie.....	301
Configurez les paramètres ISDP globaux.....	302
Configurer les paramètres ISDP d'une interface.....	303
Afficher ou effacer les informations de voisinage ISDP.....	305
Afficher ou effacer les statistiques ISDP.....	306

Chapitre 4 Configurer les informations de commutation

VLAN.....	310
Gérez la configuration VLAN sur le commutateur.....	310
Ajouter un VLAN.....	310
Modifier un VLAN.....	312
Supprimez un ou plusieurs VLAN.....	313
Réinitialisez l'ensemble de la configuration VLAN sur les paramètres par défaut.....	314
Modifiez les paramètres d'allocation VLAN internes.....	315
Présentation du réseau automatique.....	316
Activer ou désactiver les lignes de réseau automatiques.....	318
Configurez les paramètres du mode de port de commutateur pour les interfaces.....	319
Configurer les interfaces d'appartenance pour un VLAN....	322
Afficher l'état du VLAN sur le commutateur.....	324
Modifiez les paramètres de l'ID VLAN du port.....	325

Configurez un VLAN basé sur MAC.....	328
Ajoutez une configuration VLAN basée sur MAC.....	329
Supprimez une configuration VLAN basée sur MAC.....	330
Configurer un VLAN basé sur oui.....	331
Ajoutez une configuration VLAN basée sur oui.....	331
Supprimer une configuration VLAN basée sur oui.....	332
Configurer un groupe VLAN basé sur le protocole.....	333
Ajoutez un groupe VLAN basé sur le protocole.....	333
Modifier un groupe VLAN basé sur le protocole.....	335
Supprimer un groupe VLAN basé sur le protocole.....	336
Configurer les interfaces d'appartenance pour un groupe VLAN basé sur le protocole.....	337
Configurez un VLAN basé sur un sous-réseau IP.....	339
Ajoutez un VLAN basé sur un sous-réseau IP.....	339
Supprimer un VLAN basé sur un sous-réseau IP.....	340
Configurez un double VLAN.....	341
Configurer un VLAN vocal.....	343
Configurer le protocole d'enregistrement d'attribut générique.....	346
Configurer les paramètres du commutateur GARP.....	346
Configurez les paramètres GARP pour une ou plusieurs interfaces.....	347
Auto-VoIP.....	350
Configurez les paramètres basés sur le protocole Auto-VoIP..	350
Configurez les propriétés auto-VoIP basées sur oui.....	352
Configurez les paramètres de l'interface basée sur oui.....	354
Gérer la table oui	355
Ajoutez un préfixe oui.....	356
Supprimez un ou plusieurs préfixes oui.....	357
Afficher l'état Auto-VoIP	358
VLAN automatiques.....	359
Activer et configurer un VLAN de caméra automatique.....	359
Configurez une interface en tant que membre de l'VLAN de caméra automatique.....	361
Ajoutez une interface utilisateur oui pour l'Auto-Camera VLAN.....	362
Supprimez une interface utilisateur oui pour le VLAN de la caméra automatique.....	364
Activer et configurer un VLAN Auto-WiFi.....	365
Configurez une interface en tant que membre du VLAN Auto-WiFi.....	366
Ajoutez une interface utilisateur oui pour le VLAN Auto-WiFi.	367
Supprimez une interface utilisateur oui pour le VLAN Auto-WiFi.....	369

Affiche des informations sur les périphériques connectés au VLAN Auto-Camera et au VLAN Auto-WiFi.....	370
Interface Internet Small Computer System.....	371
Activez iSCSI et configurez les paramètres QoS pour le trafic iSCSI.....	372
Ajoutez une cible iSCSI.....	373
Afficher les sessions iSCSI.....	374
Afficher des informations détaillées sur les sessions iSCSI...	375
Protocole STP.....	377
Configurez les paramètres STP et affichez l'état STP	378
Configurez les paramètres CST et affichez l'état CST.....	381
Configurez les paramètres de l'interface CST.....	384
Affiche l'état de l'interface CST.....	388
Gérer les instances MST.....	390
Ajoutez une instance MST et affichez l'état MST.....	390
Modifier une instance MST.....	392
Supprimer une instance MST.....	393
Configurer et afficher les paramètres d'interface d'une instance MST.....	394
Afficher les statistiques de l'interface STP.....	397
Configurez les paramètres VLAN PVST/RPVST.....	399
Modifier une configuration VLAN PVST/RPVST.....	401
Supprimer une configuration VLAN PVST/RPVST.....	402
Configurez les paramètres d'interface PVST et RPVST.....	404
Afficher les statistiques PVST.....	406
Base de données de transfert multidiffusion.....	408
Affiche les entrées dans la base de données de transfert multidiffusion.....	408
Supprimez les entrées igmp snooping de la base de données de transfert multidiffusion.....	409
Supprimez toutes les entrées MAC multicast connues de la base de données de transfert multicast.....	410
Afficher les statistiques de la base de données de transfert multidiffusion.....	411
Surveillance du protocole de gestion de groupe Internet.....	413
Configurez igmp snooping automatiquement avec le mode IGMP plus.....	413
Configurez igmp snooping manuellement.....	415
Configurez les paramètres igmp snooping pour les interfaces.....	417
Configurez igmp snooping pour les VLAN automatiquement avec le mode IGMP plus.....	420
Configurez manuellement igmp snooping pour les VLAN...	422
Configurez une interface de routeur multidiffusion IGMP....	424
Configurez un routeur de multidiffusion IGMP VLAN	426

Présentation de l'interrogateur igmp snooping.....	427
Configurez les paramètres globaux du questeur igmp snooping.....	428
Configurer un interrogateur igmp snooping pour un VLAN ..	429
Supprimez les paramètres de requête igmp snooping pour un VLAN.....	431
Affiche l'état du demandeur igmp snooping.....	433
Surveillance de la découverte de l'écouteur multicast.....	434
Configurez la surveillance MLD automatiquement avec le mode MLD plus.....	434
Configurez manuellement la surveillance MLD.....	436
Configurez les paramètres de surveillance MLD pour les interfaces.....	438
Configurez la surveillance MLD pour les VLAN automatiquement avec le mode MLD plus.....	441
Configurez manuellement la surveillance MLD pour les VLAN.....	442
Supprimez les paramètres du questeur MLD Snooping pour un VLAN.....	444
Configurez une interface de routeur multicast MLD.....	445
Configurez un routeur de multidiffusion MLD VLAN.....	447
Configurez les paramètres globaux du questeur MLD Snooping.....	449
Configurer un interrogateur igmp snooping pour un VLAN ..	450
Supprimez les paramètres du questeur MLD Snooping pour un VLAN.....	452
Multicast VLAN Registration.....	453
Configurez les paramètres globaux du conducteur.....	454
Configurer un groupe de dossier conducteur.....	456
Supprimer un groupe de dossier du conducteur.....	457
Configurer une interface du conducteur.....	458
Configurer les membres de l'interface d'un groupe de dossier conducteur.....	460
Afficher les statistiques du dossier du conducteur.....	461
Table d'adresse MAC.....	463
Affichez, recherchez ou effacez la table d'adresses MAC....	463
Définissez l'intervalle de vieillissement des adresses dynamiques.....	465
Ajoutez une adresse MAC statique à la table d'adresses MAC.....	466
Ajoutez une adresse MAC statique à la table d'adresses MAC.....	467
Paramètres des ports.....	468
Configurez et affichez les paramètres du port.....	468
Ajoutez des descriptions de port, lag et VLAN.....	472

Affiche les informations du module émetteur-récepteur.....	474
Configurez les paramètres du volet de liaison du port.....	476
Lier les groupes d'agrégation.....	477
Présentation de Auto-lag.....	478
Activer ou désactiver les LAG automatiques.....	479
Activer ou désactiver le mode de profil AVB global Auto-lag.	480
Configurez le mode de hachage pour les LAG automatiques.	481
Configurez le mode de hachage global non unicast.....	483
Configurez les paramètres d'un lag.....	485
Configurez un lag unique et ses membres.....	488
802.1AS synchronisation et synchronisation.....	490
Configurer et afficher les paramètres 802.1AS globaux.....	491
Configurez les paramètres de l'interface 802.1AS.....	493
Afficher les statistiques 802.1AS.....	496
Protocole d'enregistrement multiple et 802.1Qav.....	498
Configurez les paramètres MRP globaux.....	499
Configurer le mappage 802.1Qav.....	502
Configurez les paramètres de l'interface MRP.....	503
Afficher ou effacer les statistiques MMRP.....	506
Afficher ou effacer les statistiques MVRP.....	508
Afficher ou effacer les statistiques du PDSF.....	510
Afficher les paramètres de réservation du PDSF.....	512
Configurer et afficher les paramètres Qav pour les interfaces.	514
Afficher les informations sur les flux PDSF.....	516
Protection contre les boucles.....	519
À propos de la protection contre les boucles.....	520
Configurez les paramètres globaux de protection contre les boucles.....	521
Configurez les paramètres de protection contre les boucles pour les interfaces et affichez l'état de protection contre les boucles.....	523

Chapitre 5 Gérer le routage

Concepts de routage.....	527
Table de routage, routes et préférences de route.....	527
Configurer une route et afficher les routes apprises.....	527
Supprimer un itinéraire.....	530
Spécifiez les préférences d'itinéraire.....	531
Routage IPv4.....	532
Gérer les paramètres de routage IPv4 globaux.....	532
Afficher les statistiques IPv4.....	534
Configurer les interfaces de routage IPv4.....	538
Supprimez l'adresse IP de routage d'une interface de routage IPv4.....	541

Configurez une adresse IP secondaire pour une interface de routage IPv4.....	543
Supprimez l'adresse IP secondaire d'une interface de routage IPv4.....	544
Routage IPv6.....	545
Gérer les paramètres de routage IPv6 globaux.....	545
Affichez la table de routage IPv6.....	547
Configurer les interfaces de routage IPv6.....	548
Configurer les paramètres de préfixe pour une interface de routage IPv6.....	552
Supprimer un paramètre de préfixe d'une interface de routage IPv6.....	554
Afficher les statistiques IPv6 et ICMPv6 pour une interface de routage IPv6.....	555
Affichez la table de voisinage IPv6 ou effacez les entrées de voisinage IPv6.....	560
Configurer les routes statiques IPv6.....	562
Supprimer une route statique IPv6.....	563
Configurez la préférence de route IPv6 pour le commutateur.	564
VLAN de routage.....	566
Créez un VLAN de routage à l'aide de l'assistant de routage statique VLAN.....	566
Configurer le routage pour un VLAN existant.....	568
Supprimez la fonction de routage d'un VLAN.....	570
Protocole de résolution d'adresse.....	571
Affiche les entrées ARP dans le cache ARP.....	572
Ajoutez ou modifiez une entrée statique dans la table ARP.	573
Supprimer une entrée ARP statique.....	575
Configurez les paramètres de la table ARP ou supprimez des entrées de la table.....	576
Protocole d'informations de routage.....	578
Activez ou désactivez le protocole RIP sur le commutateur..	579
Configurez les paramètres RIP globaux du commutateur....	580
Configurer les paramètres de l'interface RIP.....	582
Configurez les paramètres de redistribution de route RIP et affichez le résumé de redistribution de route.....	585
Découverte de routeurs et annonces de routeurs.....	588
Virtual Router Redundancy Protocol.....	590
Activez VRRP et ajoutez un routeur virtuel principal.....	591
Activez VRRP et ajoutez un routeur virtuel principal avec des paramètres améliorés.....	593
Modifiez les paramètres d'un routeur virtuel principal.....	596
Supprimez un routeur virtuel principal.....	597
Configurez un routeur virtuel secondaire.....	598
Modifiez l'adresse IP d'un routeur virtuel secondaire.....	599

Supprimez un routeur virtuel secondaire.....	600
Configurer le suivi d'interface VRRP et le suivi d'itinéraire....	601
Afficher les statistiques VRRP.....	603

Chapitre 6 Configurez OSPF et OSPFv3

Ouvrez d'abord le chemin le plus court.....	607
Activer OSPF.....	608
Configurez l'annonce de route par défaut OSPF.....	609
Configurez les paramètres OSPF globaux.....	610
Ajoutez ou supprimez un ID de zone commune OSPF.....	614
Ajoutez une zone de stub OSPF.....	616
Ajoutez une zone NSSA OSPF.....	618
Ajoutez une plage de zones OSPF.....	621
Configurez une interface OSPF.....	622
Afficher ou effacer les statistiques OSPF d'une interface....	627
Afficher ou effacer les informations de voisinage OSPF pour une interface.....	630
Affichez la base de données d'état des liens OSPF.....	632
Configurer un lien virtuel OSPF.....	635
Configurez la redistribution de route OSPF.....	639
Configurer le transfert sans arrêt OSPF.....	641
Open Shortest Path First version 3.....	643
Activer le OSPFv3.....	644
Configurez l'annonce de route par défaut OSPFv3.....	645
Configurez les paramètres OSPFv3 globaux	647
Ajouter ou supprimer un ID de zone commune OSPFv3....	650
Ajoutez une zone de stub OSPFv3.....	652
Ajoutez une zone NSSA OSPFv3.....	654
Ajoutez une plage de zones OSPFv3.....	656
Configurez une interface OSPFv3.....	658
Afficher ou effacer les statistiques OSPFv3 pour une interface.....	662
Afficher ou effacer les informations de voisinage OSPFv3 pour une interface.....	664
Affichez la base de données d'état des liens OSPFv3.....	667
Configurez une liaison virtuelle OSPFv3.....	670
Configurez la redistribution de route OSPFv3.....	673
Configurer le transfert non-stop OSPFv3.....	675

Chapitre 7 Configurer le routage multidiffusion

Routage multicast IPv4 et table de routage multicast IPv4.....	679
Affichez la table de routage multicast IPv4.....	679
Ajoutez des entrées de multidiffusion statiques à la table Mroute IPv4.....	681

Supprimez une entrée de multidiffusion statique de la table	
Mroute IPv4.....	682
Configurez les paramètres de multidiffusion globaux pour le	
commutateur.....	683
Configurer une interface multicast.....	684
Protocole DVMRP (Distance Vector Multicast Routing).....	686
Activez DVMRP sur le commutateur et affichez les informations	
d'itinéraire.....	687
Configurer une interface DVMRP.....	688
Afficher les voisins DVMRP.....	690
Afficher les sauts suivants du DVMRP.....	692
Afficher le tableau DVMRP de l'élagage.....	693
Afficher les itinéraires DVMRP.....	694
IGMP pour le routage multicast IPv4.....	696
Activer ou désactiver IGMP pour le commutateur.....	696
Configurez une interface de routage IGMP.....	697
Affiche les statistiques des interfaces de routage IGMP.....	699
Affichez les groupes IGMP et effectuez une recherche dans la	
base de données des groupes IGMP.....	701
Affichez les informations d'adhésion IGMP et effectuez une	
recherche dans la base de données d'adhésion IGMP.....	703
Configurez une interface proxy IGMP.....	705
Affiche les statistiques de l'interface proxy IGMP.....	707
Affichez l'appartenance au proxy IGMP et recherchez dans la	
base de données d'appartenance au proxy IGMP.....	708
PIM pour le routage multicast IPv4.....	710
Configurez les paramètres IPv4 PIM globaux sur le	
commutateur.....	710
Ajouter des groupes PIM-SSM IPv4.....	712
Supprimer un groupe PIM-SSM IPv4.....	713
Configurer une interface PIM IPv4.....	714
Afficher les voisins PIM IPv4 et rechercher la base de données	
des voisins PIM.....	716
Ajoutez une configuration de point de rendez-vous candidat PIM	
IPv4.....	718
Supprimer une configuration de point de rendez-vous candidat	
PIM IPv4.....	719
Configurez une interface comme candidat routeur d'amorçage	
PIM IPv4.....	720
Supprimez une configuration candidate de routeur d'amorçage	
PIM IPv4.....	721
Configurez un point de rendez-vous PIM IPv4 statique pour un	
groupe.....	723
Supprimer une configuration de point de rendez-vous PIM IPv4	
statique.....	724

Routes de multidiffusion statiques pour les adresses IPv4.....	725
Configurer des routes de multidiffusion statiques pour les adresses IPv4.....	726
Supprimer une route de multidiffusion statique pour une adresse IPv4.....	727
Limites d'administration multicast pour les adresses IPv4.....	728
Configurer une interface en tant que limite d'administration multicast.....	728
Supprimer une configuration de limite d'administration multicast pour une interface.....	730
Routage multicast IPv6 et table de routage multicast IPv6.....	731
Affichez la table de routage multicast IPv6.....	731
PIM pour le routage multicast IPv6.....	733
Configurez les paramètres IPv6 PIM globaux sur le commutateur.....	733
Ajouter des groupes PIM-SSM IPv6.....	734
Supprimer un groupe PIM-SSM IPv6.....	736
Configurer une interface PIM IPv6.....	737
Afficher les voisins PIM IPv6 et rechercher la base de données des voisins PIM.....	739
Ajoutez une configuration de point de rendez-vous candidat PIM IPv6.....	740
Supprimer une configuration de point de rendez-vous candidat PIM IPv6.....	742
Configurez une interface comme candidat routeur d'amorçage PIM IPv6.....	743
Supprimez une configuration candidate de routeur d'amorçage PIM IPv6.....	744
Configurez un point de rendez-vous PIM IPv6 statique pour un groupe.....	745
Supprimez une configuration de point de rendez-vous PIM IPv6 statique.....	747
MLD pour le routage multicast IPv6.....	748
Configurez les paramètres MLP globaux du commutateur...	748
Configurer une interface de routage MLD.....	749
Afficher les statistiques des interfaces de routage MLD.....	752
Affichez les groupes MLD et effectuez une recherche dans la base de données des groupes MLD.....	754
Afficher ou effacer les statistiques de trafic MLD.....	755
Configurer une interface proxy MLD.....	757
Afficher les statistiques de l'interface proxy MLD.....	759
Affichez l'appartenance au proxy MLD et recherchez dans la base de données d'appartenance au proxy MLD.....	760
Routes de multidiffusion statiques pour les adresses IPv6.....	762

Configurer des routes de multidiffusion statiques pour les adresses IPv6.....	763
Supprimer une route de multidiffusion statique pour une adresse IPv6.....	764

Chapitre 8 Configurer la qualité de service

Concepts de qualité de service.....	767
Classe de service.....	767
Concepts de configuration cos	767
Configurez les paramètres du mode de confiance cos globalement ou pour une interface spécifique.....	768
Mapper les priorités 802.1p aux files d'attente	770
Mappez les valeurs DSCP aux files d'attente.....	772
Configurez les paramètres de file d'attente cos pour une interface.....	773
Configurez les paramètres de file d'attente cos pour une interface.....	775
Configurez les paramètres de priorité cos WRED pour l'abandon de paquets.....	777
Services différenciés.....	780
Définition de DiffServ.....	780
Présentation de l'assistant DiffServ.....	781
Utilisez l'assistant DiffServ pour créer une classe de trafic et une stratégie pour une ou plusieurs interfaces.....	782
Configurez le mode DiffServ et affichez les entrées dans les tables MIB privées DiffServ.....	783
Configurer une classe DiffServ	785
Ajouter et configurer une classe DiffServ.....	785
Renommer une classe DiffServ existante.....	790
Modifiez les critères d'une classe DiffServ existante.....	791
Supprimer une classe DiffServ.....	792
Configurez une classe IPv6 DiffServ.....	793
Ajoutez et configurez une classe IPv6 DiffServ.....	794
Renommez une classe IPv6 DiffServ existante.....	797
Modifiez les critères d'une classe IPv6 DiffServ existante..	798
Supprimez une classe IPv6 DiffServ.....	799
Configurer une stratégie DiffServ	800
Ajouter et configurer une stratégie DiffServ.....	800
Renommer une stratégie DiffServ existante.....	806
Modifiez les attributs d'une stratégie DiffServ existante...	807
Modifier ou supprimer une classe d'une stratégie DiffServ existante.....	808
Supprimer une stratégie DiffServ.....	809
Configurez l'interface de service DiffServ	810

Attachez des stratégies DiffServ à une interface.....	810
Modifiez une ou les deux stratégies DiffServ pour une interface.....	813
Supprimez une ou les deux stratégies DiffServ d'une interface.....	814
Afficher les statistiques du service DiffServ.....	816

Chapitre 9 Gérer la sécurité du commutateur

Comptes utilisateur et mots de passe.....	820
Ajouter ou modifier un compte utilisateur.....	820
Supprimer un compte utilisateur.....	822
Configurer les exigences de mot de passe utilisateur.....	824
Activez l'authentification multifacteur sur le commutateur...	826
Modifiez le mot de passe CLI d'exécution privilégiée.....	827
Modifiez le mot de passe de la console, Telnet ou SSH.....	828
serveurs RADIUS.....	831
Configurez les paramètres globaux du serveur RADIUS.....	831
Configurez un serveur d'authentification RADIUS sur le commutateur.....	834
Ajoutez un serveur d'authentification RADIUS au commutateur.....	834
Modifiez les paramètres d'un serveur d'authentification RADIUS sur le commutateur.....	837
Supprimez un serveur d'authentification RADIUS du commutateur.....	838
Configurez un serveur d'authentification RADIUS sur le commutateur.....	839
Ajoutez un serveur de comptabilité RADIUS au commutateur.....	839
Modifiez les paramètres d'un serveur de comptabilité RADIUS sur le commutateur.....	842
Supprimez un serveur de comptabilité RADIUS du commutateur.....	843
Serveurs TACACS+.....	844
Configurez les paramètres TACACS+ globaux.....	844
Ajoutez un serveur TACACS+ au commutateur.....	846
Modifiez les paramètres d'un serveur TACACS+ sur le commutateur	848
Supprimez un serveur TACACS+ du commutateur.....	849
Listes d'authentification.....	850
Configurez une liste d'authentification de connexion.....	850
Supprimer une liste d'authentification de connexion.....	852
Configurez une liste d'activation d'authentification.....	854
Supprimez une liste d'activation d'authentification.....	856

Configurez la liste d'authentification Dot1x.....	857
Configurez la liste d'authentification HTTP.....	858
Configurez la liste d'authentification HTTPS.....	860
Sessions de connexion en cours.....	862
Accès de gestion HTTP et HTTPS.....	863
Pour configurer les paramètres d'accès HTTP :	863
Configurez les paramètres d'accès HTTPS.....	865
Message de sécurité du navigateur avec accès HTTPS.....	867
Gérer les certificats pour l'accès HTTPS	867
Afficher l'état des certificats SSL.....	868
Générez un certificat SSL.....	869
Activer un certificat.....	870
Supprimer un certificat SSL.....	871
Transférer un certificat HTTPS existant d'un serveur vers le	
commutateur.....	872
Accès de gestion SSH.....	875
Configurez les paramètres d'accès SSH globaux.....	875
Gérer les clés RSA, DSA et ECDSA pour l'accès SSH.....	877
Générez une clé RSA, DSA ou ECDSA.....	877
Supprimez une clé RSA, DSA ou ECDSA.....	879
Transférer des clés SSH existantes d'un serveur TFTP vers le	
commutateur.....	880
Accès à la gestion Telnet.....	883
Sélectionnez listes d'authentification Telnet.....	883
Configurez les paramètres Telnet entrants.....	884
Configurer les paramètres Telnet sortants.....	886
Accès à la gestion des ports de console.....	887
Déni de service.....	889
Profils et règles d'accès de gestion.....	892
Ajouter un profil d'accès	892
Ajoutez une règle au profil d'accès.....	893
Activez le profil d'accès.....	895
Afficher le résumé du profil d'accès et le nombre de paquets	
filtrés.....	896
Désactiver un profil d'accès	898
Supprimer un profil d'accès.....	899
Authentification du port.....	900
Configurez les paramètres d'authentification 802.1X	
globaux.....	900
Gérer l'authentification de port sur des ports individuels	903
Configurer les paramètres 802.1X pour un port.....	903
Initialisez 802.1X sur un port.....	908
Afficher le résumé des ports.....	910
Afficher le résumé du client.....	912
Filtres MAC pour le contrôle du trafic.....	914

Créer un filtre MAC.....	914
Supprimer un filtre MAC.....	916
Affichez le résumé du filtre MAC.....	917
Sécurité portuaire.....	919
Configurez le mode de sécurité du port global.....	919
Configurer une interface de sécurité de port.....	920
Afficher les adresses MAC apprises et les convertir en adresses statiques.....	923
Ajoutez une adresse MAC statique à la table d'adresses MAC pour la sécurité des ports.....	924
Supprimez une adresse MAC statique de la table d'adresses MAC pour la sécurité du port.....	925
Groupes de ports privés.....	927
Ajoutez un groupe de ports privés.....	927
Supprimer un groupe de ports privés.....	928
Configurer l'appartenance à un groupe de ports privés.....	929
Protection des ports.....	931
VLAN privés.....	932
Présentation des tâches de configuration Private VLAN.....	934
Attribuez un type de VLAN privé à un VLAN.....	935
Configurez une association VLAN privée avec un VLAN principal et secondaire.....	936
Supprimer une association VLAN privée existante.....	938
Configurez le mode de port VLAN privé.....	939
Interface hôte VLAN privée : Attribuez l'interface aux VLAN principaux et secondaires.....	942
Interface hôte VLAN privée : Supprimez l'interface des VLAN principal et secondaire.....	944
Interface promiscuous Private VLAN : Attribuez l'interface aux VLAN principaux et secondaires.....	946
Interface promiscuous Private VLAN : Supprimez l'interface des VLAN principal et secondaire.....	948
Interface de ligne de réseau promiscuous Private VLAN : Ajoutez des VLAN principaux et secondaires à la jonction.....	950
Interface de ligne de réseau promiscuous Private VLAN : Supprimez les VLAN principaux et secondaires de la jonction.....	952
Interface de jonction isolée Private VLAN : Ajoutez des VLAN principaux et secondaires à la jonction.....	953
Interface de jonction isolée Private VLAN : Supprimez les VLAN principaux et secondaires de la jonction.....	955
Configurez les VLAN natifs et autorisés sur une interface de jonction VLAN privée.....	956
Storm Control.....	959
Configurer les paramètres storm control globaux.....	959

Configurez les paramètres storm control pour un ou plusieurs ports.....	961
Protocole DHCP Snooping.....	964
Activez la surveillance DHCP pour le commutateur.....	964
Activez la surveillance DHCP pour un VLAN.....	965
Configurez les paramètres de l'interface de surveillance DHCP.....	967
Ajoutez une liaison DHCP statique et affichez ou effacez les liaisons DHCP dynamiques.....	969
Supprimez une liaison DHCP statique.....	971
Configurez les paramètres persistants de surveillance DHCP.	972
Afficher ou effacer les statistiques de surveillance DHCP....	973
Surveillance DHCPv6.....	975
Activez la surveillance DHCPv6 pour le commutateur.....	975
Activez la surveillance DHCPv6 pour un VLAN.....	977
Configurez les paramètres de l'interface de surveillance DHCP.....	978
Ajoutez une liaison DHCPv6 statique et affichez ou effacez les liaisons DHCPv6 dynamiques.....	980
Supprimez une liaison DHCPv6 statique.....	982
Configurer les paramètres persistants de surveillance DHCPv6.....	983
Afficher ou effacer les statistiques de surveillance DHCPv6.	984
Interfaces IP source Guard.....	986
Configurer la protection source IP sur une interface.....	986
Ajoutez une liaison IP source Guard statique et affichez ou effacez les liaisons IP source Guard dynamiques.....	988
Supprimez une liaison statique de la protection de la source IP.....	990
Interfaces de protection source IPv6.....	991
Configurer la protection source IPv6 sur une interface.....	992
Ajoutez une liaison de protection source IPv6 statique et affichez ou effacez les liaisons de protection source IPv6 dynamiques.	994
Supprimez une liaison statique IPv6 source Guard.....	996
Inspection ARP dynamique.....	997
Configurez les paramètres DAI globaux.....	997
Configurer les VLAN DAI.....	999
Configurer les interfaces DAI.....	1000
Créez une liste de contrôle d'accès DAI.....	1002
Configurez une règle pour une ACL DAI existante.....	1003
Supprimer une règle d'une liste de contrôle d'accès DAI existante.....	1004
Supprimer une liste de contrôle d'accès DAI.....	1006
Afficher les statistiques DAI.....	1007
Portail captif.....	1008

Configurez les paramètres globaux du portail captif.....	1009
Configurer un portail captif.....	1011
Supprimer un portail captif.....	1015
Configurer une liaison de portail captif.....	1016
Afficher ou supprimer des liaisons de portail captif dans la table de liaison de portail captif.....	1017
Configurer des groupes de portails captifs.....	1019
Ajouter un groupe de portails captifs.....	1019
Supprimer un groupe de portails captifs.....	1020
Configurer les utilisateurs du portail captif.....	1021
Ajouter ou modifier un compte utilisateur de portail captif.	1022
Supprimer un compte utilisateur de portail captif.....	1024
Configurez les paramètres des indicateurs de trappe de portail captif.....	1025
Afficher ou effacer les statistiques des clients du portail captif.....	1027
Liste de contrôle d'accès.....	1028
Utilisez l'Assistant ACL pour créer une ACL simple.....	1029
Utilisez l'Assistant ACL pour créer une ACL.....	1029
Modifiez une règle ACL que vous avez créée avec l'Assistant ACL.....	1033
Supprimez une règle ACL que vous avez créée avec l'Assistant ACL.....	1034
Exemple d'assistant ACL.....	1035
Configurer une ACL MAC.....	1036
Ajoutez une ACL MAC.....	1037
Modifiez le nom d'une ACL MAC.....	1038
Supprimer une ACL MAC.....	1039
Configurer les règles ACL MAC	1040
Ajoutez une règle pour une ACL MAC.....	1040
Modifier les critères de correspondance d'une règle MAC.	1043
Supprimer une règle d'une ACL MAC.....	1044
Configurer les liaisons MAC.....	1045
Affichez ou supprimez les liaisons MAC ACL dans la table de liaison MAC.....	1047
Configurer une liste de contrôle d'accès IPv4 de base ou étendue.....	1049
Ajoutez une ACL IPv4.....	1050
Modifiez le numéro ou le nom d'une liste de contrôle d'accès IPv4.....	1051
Supprimer une ACL IPv4.....	1052
Configurer des règles pour une liste de contrôle d'accès IPv4 de base	1053
Ajoutez une règle pour une ACL IPv4 de base.....	1054

Modifiez les critères de correspondance d'une règle de liste de contrôle d'accès IPv4 de base.....	1057
Supprimer une règle de liste de contrôle d'accès IPv4 de base.....	1058
Configurer des règles pour une ACL IPv4 étendue	1059
Ajoutez une règle pour une ACL IPv4 étendue.....	1059
Modifiez les critères de correspondance pour une règle ACL IPv4 étendue.....	1067
Supprimez une règle ACL IPv4 étendue.....	1068
Configurez une liste de contrôle d'accès IPv6	1069
Ajoutez une ACL IPv6.....	1069
Modifiez le nom d'une liste de contrôle d'accès IPv6....	1071
Supprimer une ACL IPv6.....	1072
Configurer des règles pour une ACL IPv6	1073
Ajoutez une règle pour une ACL IPv6.....	1073
Modifiez les critères de correspondance d'une règle ACL IPv6.....	1079
Supprimer une règle ACL IPv6.....	1080
Configurer les liaisons de l'interface ACL IP	1081
Affichez ou supprimez les liaisons IP ACL dans la table de liaison IP ACL	1083
Configurer les liaisons ACL VLAN	1084
Ajoutez une liaison ACL VLAN.....	1084
Supprimez une liaison de liste de contrôle d'accès VLAN.	1086

Chapitre 10 Surveillez le commutateur et le réseau

Statistiques des ports et des paquets EAP.....	1089
Afficher ou effacer les statistiques de port.....	1089
Afficher ou effacer les statistiques détaillées d'un port.....	1091
Afficher ou effacer les statistiques EAP et EAPOL	1098
Effectuez un test de câble	1101
Journaux.....	1102
Gérer et afficher le journal de mémoire.....	1103
Format du journal des messages.....	1105
Active ou désactive le journal de configuration des commandes.....	1106
Activer ou désactiver la journalisation de la console.....	1107
Paramètres hôte du serveur syslog et log.....	1109
Configurez les paramètres syslog.....	1109
Ajoutez un serveur syslog.....	1112
Modifiez les paramètres d'un serveur syslog.....	1113
Supprimez les paramètres d'un serveur syslog.....	1114
Journal des interruptions :.....	1115
Journaux des événements.....	1117

Configurer la journalisation USB.....	1118
Port mirroring.....	1120
VLAN RSPAN et commutateurs source et de destination.....	1123
Configurer un VLAN existant en tant que VLAN RSPAN.....	1124
Configurez le commutateur en tant que commutateur source RSPAN.....	1125
Configurez le commutateur en tant que commutateur de destination RSPAN.....	1128
Surveillance SFlow.....	1130
Présentation de l'agent sFlow.....	1130
Configurez l'interface source pour l'agent sFlow.....	1130
Configurer un récepteur sFlow.....	1132
Configurer l'interrogation et l'échantillonnage sFlow sur une interface.....	1134

Chapitre 11 Maintenance et dépannage

Enregistrez la configuration.....	1138
Installation automatique du fichier de configuration.....	1139
Configurez le processus d'installation automatique.....	1139
Option 125 serveur DHCP requis pour obtenir un fichier de configuration via l'installation automatique.....	1141
Redémarrez le commutateur à partir de l'interface utilisateur principale.....	1142
Pour rétablir les paramètres par défaut du routeur :.....	1144
Exporter un fichier à partir du commutateur	1145
Exporter un fichier du commutateur vers un serveur.....	1145
Utilisez HTTP pour exporter un fichier du commutateur vers un ordinateur.....	1148
Exportez un fichier du commutateur vers un périphérique de stockage USB.....	1150
Mettez à jour le logiciel ou téléchargez un fichier.....	1151
Télécharger un fichier logiciel ou un autre type de fichier d'un serveur vers le commutateur.....	1152
Utilisez HTTP pour télécharger un fichier logiciel ou un autre type de fichier sur le commutateur.....	1156
Télécharger un fichier logiciel ou un autre type de fichier d'un serveur vers le commutateur.....	1159
Téléchargez et installez un fichier de certificat de sécurité SSL sur le commutateur.....	1161
Gérer les images logicielles	1163
Copier une image logicielle.....	1163
Configurer les paramètres de double image	1164
Modifiez l'image logicielle qui se charge lorsque le commutateur démarre ou redémarre.....	1165

Supprimer une image logicielle.....	1166
Diagnostics et dépannage.....	1167
Envoyez une requête ping à une adresse IPv4.....	1167
Envoyez une requête ping à une adresse IPv6.....	1170
Envoyer un traceroute IPv4.....	1172
Envoyer un traceroute IPv6.....	1174
Capturer des paquets.....	1176
Effectuez un vidage mémoire complet.....	1177

Chapitre 12 Exemples de configuration

Réseaux locaux virtuels (VLAN)	1181
Exemples de configuration VLAN.....	1182
Listes de contrôle d'accès (ACL).....	1183
Exemple de configuration de l'ACL MAC.....	1184
Exemple de configuration de l'ACL IP de base.....	1185
Services différenciés (DiffServ)	1186
Classe.....	1187
Classes de trafic DiffServ.....	1188
Créer une politique.....	1188
Politique de conditionnement du trafic.....	1189
Exemple de configuration DiffServ.....	1190
Contrôle d'accès au port 802.1X.....	1192
802.1X exemple de configuration	1194
Protocole Spanning Tree multiple	1195
Exemple de configuration MSTP.....	1198
Interfaces de routage VLAN.....	1200

Annexe A Paramètres logiciels par défaut et spécifications matérielles

Accéder aux paramètres par défaut de l' interface utilisateur principale du commutateur.....	1203
Paramètres par défaut des fonctions système.....	1204
Commutation des paramètres par défaut des fonctions.....	1209
Paramètres par défaut des fonctions de routage, OSPF, OSPFv3 et multicast.....	1219
QoS propose les paramètres par défaut.....	1228
Paramètres par défaut des fonctions de sécurité.....	1229
Paramètres par défaut des fonctions de surveillance.....	1238
Spécifications techniques générales du matériel.....	1240
Spécifications techniques matérielles spécifiques au modèle.	1241
M4350-8X8F (SKU XSM4316).....	1241
M4350-12X12F (SKU XSM4324).....	1242
M4350-24G4XF (SKU GSM4328).....	1242
M4350-48G4XF (SKU GSM4352).....	1243

M4350-24X4V (SKU XSM4328CV).....	1244
M4350-24F4V (SKU XSM4328FV).....	1244
M4350-44M4X4V (SKU MSM4352).....	1245
M4350-36X4V (SKU XSM4340CV).....	1245
M4350-24X8F8V (SKU XSM4340V).....	1246
M4350-32F8V (SKU XSM4340FV).....	1246
M4350-16V4C (SKU VSM4320C).....	1247
M4350-40X4C (SKU XSM4344C).....	1247

1

Démarrez avec l'interface utilisateur principale

Ce manuel d'utilisation est destiné à la gamme NETGEAR Fully switches manageables M4350 et couvre tous les modèles de commutateurs M4350.

Ce chapitre présente la manière dont vous pouvez utiliser votre commutateur et accéder à l'interface utilisateur principale, également appelée *interface utilisateur principale*.

Ce chapitre contient les sections suivantes :

- [Publications disponibles et aide en ligne](#)
- [Commutateurs pris en charge](#)
- [Enregistrer votre produit](#)
- [Présentation de l'interface utilisateur principale et autres options de gestion](#)
- [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#)
- [Utilisez la vue périphérique dans l'interface utilisateur principale](#)
- [Configurez l'accès SNMPv3](#)
- [Découvrez et intégrez le commutateur au contrôleur NETGEAR engage](#)
- [Comment Insight et l'interface utilisateur principale interagissent l'un avec l'autre](#)
- [Informations d'identification de l'interface utilisateur principale](#)

❗ Remarque: Pour plus d'informations sur les sujets traités dans ce manuel, visitez le site Web d'assistance à l'adresse netgear.com/support.

❗ **Remarque:** Des mises à jour du micrologiciel avec de nouvelles fonctionnalités et des corrections de bugs sont disponibles de temps à autre sur netgear.com/support/download/. Certains produits vérifient régulièrement si un nouveau micrologiciel (firmware) est disponible sur le site et le télécharge, ou vous pouvez le rechercher et le télécharger manuellement. Si les fonctionnalités ou le comportement de votre produit ne correspondent pas aux éléments décrits dans ce guide, il peut être nécessaire de procéder à la mise à jour de votre micrologiciel (firmware).

Publications disponibles et aide en ligne

Vous pouvez télécharger les publications suivantes et bien plus encore pour la série NETGEAR Fully switches manageables M4350 en visitant le site netgear.com/support/download/.

- Guide d'installation
- Guide d'installation matérielle
- Manuel d'utilisation principal (ce manuel)
- Manuel de l'utilisateur Audio Video
- Notes applicatives Comment empiler les commutateurs NETGEAR M4300, qui s'applique également aux commutateurs M4350
- Foire aux questions
- Fiche technique

Lorsque vous êtes connecté à l'interface utilisateur principale, vous pouvez accéder à la documentation en ligne en sélectionnant **aide > aide en ligne > Guide de l'utilisateur**. Consultez la section [Aide en ligne de l'interface utilisateur principale](#) à la page 38.

En outre, une aide en ligne contextuelle est disponible dans l'interface utilisateur principale.

Commutateurs pris en charge

Ce manuel d'utilisation principal concerne les modèles NETGEAR Fully switches manageables série M4350 suivants :

- M4350-8X8F (SKU XSM4316)
- M4350-12X12F (SKU XSM4324)
- M4350-24G4XF (SKU GSM4328)
- M4350-48G4XF (SKU GSM4352)
- M4350-24X4V (SKU XSM4328CV)
- M4350-24F4V (SKU XSM4328FV)
- M4350-44M4X4V (SKU MSM4352)
- M4350-36X4V (SKU XSM4340CV)

- M4350-24X8F8V (SKU XSM4340V)
- M4350-32F8V (SKU XSM4340FV)
- M4350-16V4C (SKU VSM4320C)
- M4350-40X4C (SKU XSM4344C)

Enregistrer votre produit

Pour bénéficier des mises à jour et de la garantie du produit, nous vous encourageons à enregistrer votre produit. La première fois que vous vous connectez au switch, vous pouvez vous inscrire auprès de NETGEAR en cliquant sur le bouton S'inscrire maintenant.

L'enregistrement confirme que vos alertes par e-mail fonctionnent, réduit le temps de résolution du support technique et garantit l'exactitude de votre adresse de livraison. Nous aimerions également intégrer vos commentaires dans le développement futur de produits. Nous ne vendons ni ne louons jamais votre adresse e-mail et vous pouvez refuser les communications.

Pour enregistrer votre PA avec NETGEAR :

1. Visitez le site Web NETGEAR pour vous inscrire à l'adresse <https://my.netgear.com/registration/login.aspx>.
2. Cliquez sur le bouton **connexion** et suivez les instructions à l'écran pour enregistrer le switch avec votre adresse e-mail et votre mot de passe NETGEAR.

Si vous n'avez pas encore créé de compte NETGEAR, cliquez sur le lien créer un compte, suivez les instructions à l'écran pour créer un compte, puis enregistrez le commutateur avec votre adresse e-mail et votre mot de passe.

Présentation de l'interface utilisateur principale et autres options de gestion

Votre commutateur contient un serveur Web intégré et un logiciel de gestion pour la gestion et la surveillance des fonctions du commutateur. Le commutateur fonctionne comme un simple commutateur sans le logiciel de gestion. Cependant, vous pouvez utiliser le logiciel de gestion pour configurer des fonctionnalités plus avancées qui peuvent améliorer l'efficacité du commutateur et les performances globales du réseau.

Le logiciel du commutateur comprend un ensemble complet de fonctions de gestion permettant de configurer et de surveiller le système à l'aide de l'une des méthodes suivantes :

- **Interface utilisateur principale (interface utilisateur principale)** : L'interface utilisateur principale est un outil de gestion Web qui vous permet de surveiller, configurer et contrôler votre commutateur à distance à l'aide d'un navigateur Web standard. Vous pouvez accéder à l'interface utilisateur principale via un port réseau Ethernet ou via le port hors bande (OOB) (également appelé port de service). Depuis votre navigateur Web, vous pouvez surveiller les performances de votre commutateur et optimiser sa configuration pour votre réseau. Vous pouvez configurer toutes les fonctionnalités de commutateur disponibles, telles que les VLAN, les QoS et les listes de contrôle d'accès, à l'aide de l' interface utilisateur principale.

Ce manuel décrit comment utiliser l'interface utilisateur du périphérique pour gérer et surveiller le commutateur.

- **Interface utilisateur audio-vidéo (AV UI)** : L'interface utilisateur AV est un outil de gestion basé sur le Web qui vous permet de configurer et d'appliquer des profils réseau à des sites et de configurer de nombreuses fonctionnalités avancées pouvant améliorer les flux AV, l'efficacité des commutateurs et les performances globales du réseau. Vous pouvez accéder à l'interface utilisateur AV via un port réseau Ethernet ou via le port OOB.

Pour plus d'informations, reportez-vous au *Manuel de l'utilisateur Audio vidéo* , que vous pouvez télécharger en visitant le site netgear.com/support/download et en saisissant votre numéro de modèle dans la zone de recherche.

- **Application NETGEAR engage Controller** : L'application NETGEAR engage Controller vous permet de détecter, d'intégrer, de gérer et de surveiller le commutateur dans un réseau AV ou un autre type de réseau d'entreprise.

Pour plus d'informations, voir Découvrez et intégrez le commutateur au contrôleur NETGEAR engage à la page 43, Informations d'identification de l'interface utilisateur principale à la page 46 et le *Manuel de l'utilisateur du contrôleur engage* , que vous pouvez télécharger en visitant le site netgear.com/support/download et en saisissant votre numéro de modèle dans la zone de recherche.

- **NETGEAR Insight** Le portail cloud Netgear insight et App Insight vous permettent de découvrir, d'intégrer, de gérer et de surveiller le switch dans un réseau Insight.

❗ Remarque: Netgear insight et l'application engager le contrôleur s'excluent mutuellement. Pour changer le mode de gestion du commutateur de Insight à contrôleur d'engagement, ou inversement, réinitialiser le commutateur aux réglages par défaut d'usine.

Pour plus d'informations sur les abonnements Netgear insight, visitez netgear.com/business/services/insight/ et kb.netgear.com/000061848.

Ce manuel ne décrit pas les procédures Netgear insight, qui sont documentées dans la base de connaissances NETGEAR. Pour obtenir des articles de la base de connaissances sur Netgear insight, visitez le [site kb.netgear.com/000044338/](http://kb.netgear.com/000044338/).

- **Protocole SNMP (simple Network Management Protocol)** : SNMP est activé par défaut. Le commutateur utilise à la fois des MIB publiques standard pour la fonctionnalité standard et des MIB privées qui prennent en charge des fonctionnalités de commutateur supplémentaires. Toutes les MIB privées commencent par un préfixe "-". L'objet principal pour la configuration de l'interface se trouve dans la MIB Netgear SmartSwitch, qui est une MIB privée. Certaines configurations d'interface impliquent également des objets dans la MIB publique, IF-MIB.
- **Interface de ligne de commande (CLI)** : L'interface de ligne de commande est un moyen textuel de gérer et de surveiller le commutateur. Vous pouvez accéder à la CLI à l'aide d'une connexion série directe ou d'une connexion logique distante avec Telnet ou SSH. Pour plus d'informations sur l'interface CLI, reportez-vous au *Manuel de référence des commandes CLI*, que vous pouvez télécharger prochainement en visitant le site netgear.com/support/download et en saisissant votre numéro de modèle dans la zone de recherche.

Chacune des méthodes de gestion normalisées vous permet de configurer et de surveiller les composants du commutateur. La méthode que vous utilisez pour gérer le système dépend de la taille et des exigences de votre réseau, ainsi que de vos préférences.

Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web

Vous pouvez utiliser un navigateur Web pour accéder au commutateur et vous connecter. Vous devez pouvoir envoyer une requête ping à l'adresse IP de l'interface de gestion (n'importe quel port réseau Ethernet) ou au port hors bande (OOB) de votre ordinateur pour que l'accès Web soit disponible :

- **Interface d'administration** Par défaut, le client DHCP de l'interface de gestion est activé pour que l'interface puisse recevoir une adresse IP d'un serveur DHCP de votre réseau.

Si l'interface de gestion ne reçoit pas d'adresse IP d'un serveur DHCP, l'adresse IP par défaut de l'interface est définie sur 169.254.100.100 avec 255.255.0.0 comme

masque de sous-réseau. Il en va de même si vous connectez le port OOB directement à un ordinateur et redémarrez le commutateur.

- **Port OOB** : Par défaut, le client DHCP du port OOB est activé pour que le port puisse recevoir une adresse IP d'un serveur DHCP de votre réseau.

Si le port OOB ne reçoit pas d'adresse IP d'un serveur DHCP de votre réseau, l'adresse IP du port est définie sur 192.168.0.239 avec 255.255.0.0 comme masque de sous-réseau. Il en va de même si vous connectez le port OOB directement à un ordinateur et redémarrez le commutateur.

Si vous laissez un serveur DHCP de votre réseau attribuer une adresse IP au commutateur, déterminez l'adresse IP en accédant au serveur DHCP ou en utilisant un utilitaire de scanner IP.

Pour plus d'informations sur la première connexion au commutateur, reportez-vous aux informations du guide d'installation.

❗ Remarque: La première fois que vous vous connectez en tant qu'administrateur à l'interface utilisateur principale, aucun mot de passe n'est requis (c'est-à-dire que le mot de passe est vide). Après vous être connecté pour la première fois, vous devez spécifier un mot de passe de périphérique local que vous devrez utiliser chaque fois que vous vous connecterez (vous pourrez modifier à nouveau le mot de passe).

Connectez-vous à l'interface utilisateur principale à l'aide de l'adresse IP par défaut du commutateur

Pour utiliser l'adresse IP par défaut du commutateur pour accéder au commutateur via l'interface utilisateur principale :

1. Configurez votre ordinateur avec une adresse IP statique.
 - Pour un accès via un port réseau Ethernet, utilisez une adresse IP dans le sous-réseau 169.254.0.0 avec le masque de sous-réseau 255.255.0.0.
Par exemple, utilisez 169.254.100.201 pour votre ordinateur.
 - Pour un accès via le port OOB, utilisez une adresse IP dans le sous-réseau 192.168.0.0 avec le masque de sous-réseau 255.255.0.0.
Par exemple, utilisez 169.254.100.201 pour votre ordinateur.
2. Connectez un câble Ethernet entre le port Ethernet de votre ordinateur et un port réseau Ethernet ou le port OOB du switch.

3. Si vous utilisez le port OOB, redémarrez le commutateur de sorte que l'adresse IP du port OOB soit définie sur 192.168.0.239 avec 255.255.255.0 comme masque de sous-réseau.
4. Lancez un navigateur Web tel que Google Chrome, Mozilla Firefox ou Microsoft Internet Explorer.
5. Saisissez l'adresse IP par défaut du switch dans le champ d'adresse du navigateur :
 - Pour accéder via un port réseau Ethernet, saisissez **169.254.100.100**.
 - Pour un accès via le port OOB, saisissez **192.168.0.239**.

La page de connexion s'affiche.

6. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

7. Entrez **admin** comme nom d'utilisateur, entrez le mot de passe de votre périphérique local, puis cliquez sur le bouton **connexion**.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

La page System Information (Informations système) s'affiche.

Connectez-vous à l'interface utilisateur principale avec une adresse IP connue

Si vous n'avez pas attribué d'adresse IP statique au commutateur mais que vous avez laissé un serveur DHCP de votre réseau attribuer une adresse IP au commutateur, déterminez l'adresse IP en accédant au serveur DHCP ou en utilisant un utilitaire de scanner IP.

Les procédures décrites dans ce manuel supposent que vous connaissez l'adresse IP de votre commutateur.

Pour utiliser une adresse IP connue pour accéder au commutateur via l'interface utilisateur principale :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

Principaux boutons de l'interface utilisateur et champs définis par l'utilisateur

Le tableau suivant présente les boutons de commande utilisés dans les pages de l'interface utilisateur du périphérique.

Table 1 : Boutons de commande de l'interface utilisateur principale

Bouton	Function (Fonction).
Ajouter	Cliquez sur le bouton Ajouter pour ajouter le nouvel élément configuré dans la ligne d'en-tête d'un tableau.
Appliquer	Cliquez sur le bouton appliquer pour envoyer la configuration mise à jour au commutateur. Les modifications apportées à la configuration prennent effet immédiatement.
Annuler	Cliquer sur le bouton Annuler annule la configuration de la page et réinitialise les données de la page aux valeurs précédentes du commutateur.
Delete (Suppression)	Cliquez sur le bouton Supprimer pour supprimer l'élément sélectionné.
Actualiser	Cliquez sur le bouton Actualiser pour actualiser la page avec les dernières informations du périphérique.
Enregistrer	Cliquez sur le bouton Enregistrer pour enregistrer vos paramètres. Il se trouve dans le coin supérieur droit de l'interface utilisateur du périphérique.
Déconnexion	Cliquez sur le bouton déconnexion pour mettre fin à la session. Il se trouve dans le coin supérieur droit de l'interface utilisateur du périphérique.

Les champs configurables peuvent contenir de 1 à 159 caractères, sauf indication contraire sur la page Web de configuration. Tous les caractères peuvent être utilisés, à l'exception des caractères suivants (sauf indication contraire dans pour cette fonction) :

Table 2 : Caractères non valides pour les champs définis par l'utilisateur

Caractères non valides pour les champs définis par l'utilisateur

\ | / < > * ?

Conventions de dénomination des interfaces

Le commutateur prend en charge les interfaces physiques et logiques. Les interfaces sont identifiées par leur type et leur numéro. Les ports physiques sont des interfaces Ethernet multivitesse ou des ports fibre optique et sont numérotés sur le panneau avant. Vous configurez les interfaces logiques.

Le tableau suivant décrit la convention de dénomination de toutes les interfaces disponibles sur le commutateur.

Table 3 : Conventions de dénomination des interfaces

Interface	Description	Exemple
Interfaces physiques	Selon le modèle de commutateur, les ports physiques sont des ports Ethernet 10G multivitesse, des ports Ethernet 2.5G multivitesse, des ports Gigabit Ethernet, des ports fibre 25G, des ports fibre 10G ou une combinaison de ces ports. Le numéro d'interface se compose du numéro d'unité de commutation (de 1 à 8) suivi d'une barre oblique, du numéro d'emplacement (toujours 0) suivi d'une barre oblique et du numéro de port, qui est un numéro séquentiel commençant par 1.	1/0/1, 1/0/2, 1/0/3, etc Pour une pile de commutateurs : 2/0/1, 2/0/2, 2/0/3, etc 3/0/1, 3/0/2, 3/0/3, etc
Groupes d'agrégation de liaisons (LAG)	Une interface lag est une interface logique qui regroupe deux ports physiques ou plus.	lag 1, lag 2, lag 3, etc
Interface de gestion CPU	Il s'agit de l'interface interne du commutateur responsable de l'adresse MAC de base du commutateur. Cette interface n'est pas configurable et est toujours répertoriée dans le tableau des adresses MAC.	0/5/1
Interfaces VLAN de routage	Il s'agit d'une interface utilisée pour la fonctionnalité de routage.	VLAN 1, VLAN 2, VLAN 3, etc

Enregistrez vos paramètres dans la configuration en cours

Lorsque vous cliquez sur le bouton **appliquer**, vos modifications sont enregistrées pour la session de gestion Web mais ne sont pas conservées lorsque vous redémarrez le commutateur. Pour enregistrer les modifications apportées à la configuration en cours (c'est-à-dire de manière permanente), cliquez sur l'icône **Enregistrer** en haut à droite d'une page.

Vous pouvez également effectuer plusieurs modifications sans cliquer sur l'icône **Enregistrer** après chaque modification (bien que vous devez cliquer sur le bouton **appliquer** après chaque modification), puis enregistrer la configuration dans la configuration en cours. (Pour plus d'informations, consultez la section Enregistrez la configuration à la page 1138.)

Aide en ligne de l'interface utilisateur principale

Lorsque vous vous connectez au commutateur, chaque page contient un lien vers l'aide en ligne () qui contient des informations pour vous aider à configurer et à gérer le commutateur. Les fenêtres contextuelles de l'aide en ligne sont contextuelles. Par exemple, si la page adresse IP est ouverte, la rubrique d'aide de cette page s'affiche si vous cliquez sur le bouton aide.

Vous pouvez vous connecter au site d'assistance en ligne à l'adresse netgear.com/support lorsque vous êtes connecté au commutateur.

Pour accéder au lien d'assistance en ligne :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **aide > aide en ligne > support**.

6. Pour vous connecter au site d'assistance NETGEAR pour les commutateurs de la série M4250, cliquez sur le bouton **appliquer**.

Utilisez la vue périphérique dans l'interface utilisateur principale

La vue périphérique est une applet HTML qui affiche les ports sur le commutateur. Cet outil graphique offre une autre façon de naviguer vers les options de configuration et de surveillance. L'outil graphique fournit également des informations sur les ports de périphériques, la configuration et l'état, les tables et les composants de fonctionnalités.

Pour utiliser la vue périphérique :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur principale à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez système > affichage du périphérique.

La vue avant du commutateur de la vue périphérique s'affiche. Si une pile est configurée, la vue avant de chaque commutateur empilé s'affiche.

La couleur du port indique l'état du port :

- **Noir** Le port est désactivé ou n'est pas connecté à un périphérique.
- **Vert** : Le port est connecté à un périphérique.
- **Gris**. Le port est détaché. Par exemple, un port est détaché si informatique est configuré en tant que port de pile mais n'est pas connecté à un membre de pile.
- **Rouge** : Une erreur s'est produite sur le port.

Les voyants du port indiquent l'état du port et les voyants du système indiquent l'état du système. Pour plus d'informations sur ces conditions, reportez-vous au guide d'installation matérielle, que vous pouvez télécharger en vous rendant sur le site [.netgear.com/support/download/](http://netgear.com/support/download/)

6. Pour afficher la vue arrière, cliquez sur le bouton **B**, et pour afficher à nouveau la vue avant, cliquez sur le bouton **F**.

Si la vue avant s'affiche, le bouton B s'affiche pour vous permettre de passer à la vue arrière. Si la vue arrière s'affiche, le bouton F s'affiche pour vous permettre de passer à la vue avant.

7. Pour afficher les menus qui vous permettent de configurer les ports, pointez sur un port et cliquez dessus avec le bouton droit de la souris.

À l'aide du menu de la vue périphérique, vous pouvez naviguer jusqu'à une page et configurer les paramètres du port.

8. Pour afficher les menus qui vous permettent de configurer les paramètres globaux du commutateur, pointez sur n'importe quel point du commutateur autre qu'un port, puis cliquez avec le bouton droit de la souris.

À l'aide du menu de la vue périphérique, vous pouvez naviguer jusqu'à une page et configurer les paramètres du commutateur.

Configurez l'accès SNMPv3

Le commutateur prend en charge la configuration des groupes SNMP et des utilisateurs qui peuvent gérer les interruptions générées par l'agent SNMP.

Le commutateur utilise à la fois des MIB publiques standard pour la fonctionnalité standard et des MIB privées qui prennent en charge des fonctionnalités de commutateur supplémentaires. Toutes les MIB privées commencent par un préfixe "-". L'objet principal pour la configuration de l'interface se trouve dans la MIB Netgear SmartSwitch, qui est une MIB privée. Certaines configurations d'interface impliquent également des objets dans la MIB publique, IF-MIB.

SNMP est activé par défaut. La page informations système, qui s'affiche lorsque vous vous connectez, affiche les informations dont vous avez besoin pour configurer un gestionnaire SNMP pour accéder au commutateur.

Vous ne pouvez pas accéder au commutateur à l'aide de SNMPv3 tant que vous n'êtes pas connecté au commutateur en tant qu'administrateur et que vous n'avez pas modifié le mot de passe par défaut (voir [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33). Ensuite, SNMPv3 est automatiquement configuré avec le protocole d'authentification SHA512 et le nouveau mot de passe de l'utilisateur admin.

Pour l'accès au commutateur SNMPv3, le protocole d'authentification doit être SHA512.

Pour obtenir plus d'informations sur les volumes, consultez la section .

Pour configurer les paramètres d'authentification et de cryptage du profil administrateur SNMPv3 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez System > SNMP > SNMP V1/V3 > Community Configuration.

La page Configuration utilisateur s'affiche.

6. Dans le menu **Protocole d'authentification**, sélectionnez **SHA512** pour l'authentification.

SHA512 est le seul choix possible dans le menu.

7. Dans le champ **Authentication Key** (clé d'authentification), saisissez un mot de passe (clé).

Le mot de passe peut comporter jusqu'à 32 caractères.

8. Dans le menu **Protocole de cryptage**, sélectionnez **aucun** ou **AES128** pour le cryptage :

- **Aucun** : Les informations ne sont pas cryptées.
- **AES128** : Vous devez spécifier un mot de passe de cryptage pour l'accès SNMPv3 (voir l'étape suivante).

9. Si vous sélectionnez **AES128** dans le menu **Encryption Protocol**, spécifiez un mot de passe (clé) dans le champ **Encryption Key**.

Le mot de passe peut comporter jusqu'à 32 caractères.

10. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

11. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

❗ Remarque: Pour plus d'informations sur l'utilisation de SNMPv1 ou SNMPv2, reportez-vous à la section [Simple Network Management Protocol](#) à la page 257.

Découvrez et intégrez le commutateur au contrôleur NETGEAR engage

Vous pouvez utiliser l'application NETGEAR engage Controller pour découvrir, intégrer, gérer et surveiller le commutateur. L'application NETGEAR engage Controller (appelée *contrôleur* dans cette section) permet de centraliser la gestion et la configuration des commutateurs et autres périphériques pris en charge via une application portable compatible audio-vidéo (AV) pour Windows et MacOS.

❗ Remarque: Cette section fait référence à une configuration dans laquelle le contrôleur est déjà installé. Pour télécharger et installer le contrôleur, reportez-vous aux informations du *Manuel de l'utilisateur du contrôleur engage*, que vous pouvez télécharger en visitant le Centre de téléchargement NETGEAR à l'adresse netgear.com/support/download.

Pour découvrir et intégrer le commutateur au contrôleur :

1. Sur votre ordinateur, dans le dossier dans lequel vous avez installé l'application de contrôleur, double-cliquez sur l'icône de l'application **Engage** ou sur le raccourci **Engage**.
La fenêtre de connexion s'ouvre.
2. Dans le champ **Login Name** (Nom de connexion), saisissez le nom d'utilisateur **admin**.
3. Dans le champ **mot de passe**, entrez le mot de passe du contrôleur que vous avez configuré la première fois que vous vous êtes connecté.
4. Cliquez sur le bouton **Login** (Connexion)
La page Managed Devices (Appareils gérés) s'affiche.
5. Si vous configurez plusieurs sites, procédez comme suit :
 - a. Dans le menu **Site**, sélectionnez le site.
 - b. Dans la fenêtre contextuelle modifier la configuration du réseau, confirmez que les paramètres d'adresse IP et engagez l'interface réseau pour le site sont toujours corrects en cliquant sur le bouton **appliquer**.
Vous pouvez également modifier les paramètres d'adresse IP et activer l'interface réseau Engage du site.
6. Selon que le commutateur s'affiche ou non dans le tableau périphériques découverts, effectuez l'une des opérations suivantes :

- **Le commutateur affiche dans le tableau périphériques découverts** : Cliquez sur le bouton **Onboard** du commutateur pour afficher la fenêtre contextuelle Onboard.
 - **Le commutateur ne s'affiche pas dans le tableau périphériques découverts** : Cliquez sur le lien **Ajouter un périphérique** pour afficher la fenêtre contextuelle Ajouter un périphérique.
7. Pour permettre au contrôleur d'intégrer le commutateur afin qu'il puisse contrôler le commutateur, spécifiez les informations suivantes :
- **Device Password** (Mot de passe de l'appareil) : Saisissez le mot de passe du périphérique local pour le commutateur.
Si le commutateur est à l'état usine par défaut, cliquez sur la bascule **utiliser le mot de passe par défaut du périphérique** pour qu'il s'affiche en vert et se trouve à droite.
 - **Device IP Address** (Adresse IP de l'appareil) : Si l'adresse IP n'est pas répertoriée, saisissez l'adresse IP du commutateur.
- ❗ **Remarque:** Par défaut, *admin* s'affiche dans le champ Device Admin User (Utilisateur administrateur de l'appareil).
8. Utilisez l'une des méthodes suivantes en fonction de la fenêtre qui s'affiche :
- Dans la fenêtre Onboard (Intégrer), cliquez sur le bouton **Apply** (Appliquer).
 - Dans la fenêtre Add Devices (Ajouter des appareils), cliquez sur le bouton **Add** (Ajouter).
- Les paramètres sont enregistrés.
9. Pour enregistrer les paramètres dans la configuration en cours d'exécution, cliquez sur le bouton **Save** (Enregistrer) en haut à droite de la page.
- Vous pouvez maintenant gérer et surveiller le commutateur à l'aide du contrôleur. Pour plus d'informations, consultez le *Manuel de l'utilisateur du contrôleur Engage*.

- ❗ **Remarque:** Après avoir intégré le commutateur à un site engage, le mot de passe du site engage remplace le mot de passe de l'appareil local du commutateur pour l'interface utilisateur principale. Pour accéder à l'interface utilisateur principale, vous devez saisir le mot de passe du site engage.

Comment Insight et l'interface utilisateur principale interagissent l'un avec l'autre

si vous gérez le switch à l'aide du portail Insight Cloud ou de l'application Insight, vous pouvez toujours gérer le switch à l'aide de son interface utilisateur. Cela signifie que ces méthodes de gestion ne s'excluent pas mutuellement, mais se complètent. Les modifications apportées dans Insight sont synchronisées avec l'interface utilisateur de l'appareil. Inversement, les modifications apportées dans l'interface utilisateur de l'appareil sont synchronisées avec Insight.

❗ Remarque: La synchronisation entre l'interface utilisateur principale et Insight peut prendre jusqu'à 15 minutes. Pendant la période de synchronisation, n'effectuez pas les mêmes modifications sur l'interface utilisateur principale et sur Insight ou des modifications conflictuelles sur l'interface utilisateur principale et sur Insight.

Par défaut, Netgear insight est activé mais inactif si vous ne configurez pas et n'utilisez pas informatique. Si Insight est inactif, les modifications apportées à l'interface utilisateur principale ne sont pas synchronisées avec Insight. Vous ne pouvez pas utiliser l'interface utilisateur principale pour désactiver Insight. Toutefois, si vous ne configurez pas et n'utilisez pas Insight, informatique est effectivement désactivé.

❗ Remarque: Netgear insight et l'application engager le contrôleur s'excluent mutuellement.

limité

Netgear insight ne prend pas en charge les fonctionnalités suivantes, que vous pouvez configurer dans l'interface utilisateur principale :

- serveurs SNTP
- Mode de routage IP
- Configuration de l'VLAN du MLD

En outre, Netgear insight ne prend pas en charge les paramètres spécifiques pour les fonctionnalités suivantes, qui sont entièrement configurables dans l'interface utilisateur principale :

- Les paramètres globaux PoE sont pris en charge, à l'exception du seuil d'utilisation du système et du mode de gestion de l'alimentation
- Les paramètres de port PoE sont pris en charge, à l'exception de la priorité de port

- Voice VLAN est pris en charge, à l'exception du mode d'interface de port et de la valeur de port
- La VoIP automatique est prise en charge, mais seule la table oui par défaut (pas d'oui personnalisée)
- STP est pris en charge, mais pas MSTP
- Le routage VLAN est pris en charge, mais pas une MTU IP configurable
- La configuration de route est prise en charge, sauf pour la préférence de route et la description de route
- La configuration de l'interface cos est prise en charge, à l'exception de la vitesse de mise en forme de l'interface
- Les serveurs RADIUS sont pris en charge, à l'exception de la configuration du serveur de comptabilité RADIUS
- Le contrôle du trafic est pris en charge, à l'exception de la configuration du filtre MAC et des paramètres de sécurité des ports
- Les configurations ACL sont prises en charge, mais pas l'Assistant ACL
- L'exportation de fichiers HTTP est prise en charge, mais pas pour une configuration texte ; la mise à niveau de fichiers HTTP est prise en charge, mais pas pour une configuration texte

Vous pouvez configurer ces fonctionnalités dans l'interface utilisateur principale.

Informations d'identification de l'interface utilisateur principale

Les informations contenues dans cette section font référence au mot de passe du périphérique local que vous devez utiliser lorsque vous accédez à l'interface utilisateur principale du commutateur.

La première fois que vous accédez à l'interface utilisateur du périphérique, entrez le mot de passe administrateur par défaut (password), après quoi vous devez personnaliser le mot de passe pour plus de sécurité. Chaque fois que vous vous connectez à l'interface utilisateur du terminal, utilisez votre mot de passe administrateur personnalisé.

Si vous intégrez le commutateur à l'application contrôleur d'engagement NETGEAR, puis ajoutez le commutateur à un site contrôleur d'engagement, le mot de passe du périphérique local devient le *mot de passe du site* contrôleur d'engagement .

Si vous ajoutez le commutateur à un réseau Netgear insight, le mot de passe du périphérique local devient le *mot de passe du réseau* Insight .

Pour plus d'informations sur le fonctionnement du mot de passe réseau Insight et pour consulter des articles de la base de connaissances sur Netgear insight, visitez le site kb.netgear.com/000044338/.

Le tableau suivant répertorie les options d'informations d'identification pour l'accès à l'interface utilisateur du périphérique en relation avec le contrôleur d'engagement.

Table 4 : Informations d'identification pour l'accès à l'interface utilisateur principale en relation avec le contrôleur engage

Intégré à un site engage Controller	Informations d'identification	Menu principal
Aucun	Mot de passe du périphérique local	Menu principal complet de l'interface utilisateur
Oui	Mot de passe du site du contrôleur d'engagement	Menu principal complet de l'interface utilisateur
D'abord ajouté à un site, puis supprimé du site et du contrôleur	Engagez le mot de passe du site du contrôleur jusqu'à ce que vous définissiez un nouveau mot de passe de périphérique local	Menu principal complet de l'interface utilisateur

Le tableau suivant répertorie les options d'informations d'identification essentielles pour l'accès à l'interface utilisateur du périphérique en relation avec Netgear insight.

Table 5 : Informations d'identification pour l'accès à l'interface utilisateur principale par rapport à Insight

Ajouté à un réseau Insight	Informations d'identification	Menu principal
Aucun	Mot de passe du périphérique local	Menu principal complet de l'interface utilisateur
Oui	Mot de passe réseau Insight	Menu principal complet de l'interface utilisateur
D'abord ajouté à un réseau Insight, puis supprimé du réseau mais pas ajouté à un autre réseau Insight.	Mot de passe réseau Insight jusqu'à ce que vous définissiez un nouveau mot de passe de périphérique local	Menu principal complet de l'interface utilisateur

❗ Remarque: Netgear insight et l'application engager le contrôleur s'excluent mutuellement.

2

Gérer la superposition

Ce chapitre aborde les sujets suivants :

- Présentation de l'empilement des commutateurs
- Synchronisation et mise à niveau du micrologiciel de pile
- Maintenance de la configuration de la pile
- Sélection du commutateur de gestion de pile
- Comportement de réinitialisation par défaut de la pile
- Limites d'empilement
- Configurer une pile
- Transfert continu de pile

Présentation de l'empilement des commutateurs

Un commutateur empilable est un commutateur entièrement fonctionnel fonctionnant comme une unité autonome, mais qui peut également fonctionner avec jusqu'à sept autres commutateurs. Ce groupe de commutateurs a les caractéristiques d'un commutateur unique et la capacité de port de la somme de tous les commutateurs empilés.

L'un des commutateurs de la pile commande le fonctionnement de la pile. Ce commutateur est appelé commutateur de gestion de pile. Les autres commutateurs de la pile sont des membres de pile. Le commutateur de gestion de pile et les membres de pile utilisent la technologie d'empilement pour se comporter et travailler ensemble comme un système unifié. Les protocoles de couche 2 et supérieurs présentent l'ensemble de la pile de commutateurs comme une seule entité du réseau.

Une pile de commutateurs peut être décrite en termes de trois fonctions semi-indépendantes :

- **Plan de transfert** : Le plan de transfert transfère les paquets de données. Le plan de transfert est implémenté dans le matériel.
- **Plan de contrôle** : Le plan de contrôle est l'ensemble des protocoles qui déterminent comment le plan de transfert transfère les paquets, c'est-à-dire quels paquets peuvent être transférés et où ils vont. Le logiciel d'application sur le commutateur de gestion agit comme le plan de contrôle.
- **Plan de gestion** : Le plan de gestion est un logiciel d'application exécuté sur le commutateur de gestion qui fournit les interfaces, vous permettant de configurer et de surveiller la pile de commutateurs.

Le commutateur de gestion de pile est le point unique de gestion de pile. À partir du commutateur de gestion de pile, vous configurez les éléments suivants :

- Fonctionnalités de niveau système (globales) qui s'appliquent à tous les membres de la pile
- Fonctionnalités au niveau de l'interface pour toutes les interfaces sur n'importe quel membre de la pile

Une pile de commutateurs est identifiée dans le réseau par son adresse IP réseau. L'adresse IP du réseau est attribuée en fonction de l'adresse MAC du commutateur de gestion de pile. Chaque membre de la pile est identifié de manière unique par son propre numéro de membre de la pile, qui est un nombre compris entre 1 et 8. Le commutateur de gestion de pile peut être n'importe quel nombre dans cette plage.

L'empilage prend en charge les éléments suivants :

- Jusqu'à huit commutateurs par pile
- Gestion d'une adresse IP unique via un navigateur Web, l'interface de ligne de commande ou SNMP
- Configuration des membres du commutateur de gestion :
 - Le commutateur de gestion de pile conserve la configuration pour l'ensemble de la pile.
 - Détection automatique des nouveaux membres, avec synchronisation du firmware (mise à niveau ou rétrogradation, selon les besoins)
- Mises à jour de configuration dans la pile en une seule opération
- Basculement automatique du commutateur de gestion. Pile entièrement résiliente avec topologie en anneau ou topologie de colonne vertébrale et de feuille.
- Remplacement à chaud (insertion et retrait) des éléments de pile.

Synchronisation et mise à niveau du micrologiciel de pile

Tous les membres de la pile doivent exécuter la même version de micrologiciel pour assurer la compatibilité au sein de la pile. Par défaut, si un commutateur est ajouté à la pile et que sa version de micrologiciel est différente de celle du commutateur de gestion de pile, ce commutateur ne peut pas rejoindre la pile. Vous pouvez activer la fonction mise à niveau automatique du micrologiciel de pile pour synchroniser automatiquement la version du micrologiciel du nouveau commutateur avec la version exécutée sur le commutateur de gestion de pile. L'opération de synchronisation peut entraîner une mise à niveau ou une rétrogradation du micrologiciel sur le membre de pile non concordant.

La mise à niveau du micrologiciel sur une pile de commutateurs est identique à la mise à niveau du micrologiciel sur un seul commutateur. Après avoir téléchargé le micrologiciel (voir [Mettez à jour le logiciel ou téléchargez un fichier](#) à la page 1151), le micrologiciel téléchargé est distribué à tous les commutateurs connectés de la pile. Si vous configurez une nouvelle pile, nous vous recommandons d'abord de mettre à niveau le micrologiciel sur le commutateur de gestion de pile, puis d'ajouter les membres de la pile.

❗ Remarque: Nous vous recommandons de définir le micrologiciel actif pour tous les membres de la pile de la même manière que le micrologiciel actif du commutateur de gestion de pile. En d'autres termes, si l'image 1 est l'image active sur le commutateur de gestion de pile, tous les commutateurs doivent utiliser l'image 1 comme image active. Pour plus d'informations sur la configuration de l'image active, reportez-vous à la section Modifiez l'image logicielle qui se charge lorsque le commutateur démarre ou redémarre à la page 1165.

Maintenance de la configuration de la pile

Le commutateur de gestion de pile stocke et conserve les fichiers de configuration enregistrés et en cours d'exécution pour la pile de commutateurs. Les fichiers de configuration incluent les paramètres de niveau système pour la pile de commutateurs et les paramètres de niveau interface pour tous les membres de la pile. Chaque membre de la pile conserve une copie du fichier enregistré à des fins de sauvegarde. Si le commutateur de gestion est supprimé de la pile ou devient indisponible, un autre membre est élu commutateur de gestion et s'exécute à partir de cette configuration enregistrée.

Le commutateur de gestion de pile copie sa configuration en cours sur le membre de pile configuré comme unité de secours chaque fois que le informatique change (sous réserve de certaines restrictions visant à réduire la surcharge). Ceci permet à l'unité de secours de prendre en charge le fonctionnement de la pile avec une interruption minimale si le commutateur de gestion de pile devient indisponible. La synchronisation running-config se produit également lorsque la configuration en cours est automatiquement enregistrée sur le commutateur de gestion de pile ou lorsque l'unité de secours change.

Sélection du commutateur de gestion de pile

Tous les membres de la pile sont des commutateurs de gestion de pile éligibles. Si le commutateur de gestion de pile devient indisponible, les membres de pile restants participent à l'élection d'un nouveau commutateur de gestion de pile parmi eux. Les

facteurs suivants déterminent quel commutateur est choisi comme commutateur de gestion de pile :

- Rôle actuel : Le commutateur qui est le commutateur de gestion a toujours la priorité pour conserver le rôle de commutateur de gestion.
- Priorité attribuée
- adresse MAC

Lorsque la pile est mise sous tension et que le processus d'amorçage est terminé ou que le commutateur de gestion de pile d'origine devient indisponible, le commutateur de gestion de pile est déterminé par un processus de sélection.

Les règles pour l'élection de commutateur de gestion de pile sont les suivantes :

- Si une unité a été précédemment élue commutateur de gestion de pile, informatique reste le commutateur de gestion de pile et les autres unités sont des membres de pile.
- Si aucune unité n'était un commutateur de gestion de pile, ou si plusieurs unités étaient un commutateur de gestion de pile, alors l'unité avec la priorité de gestion la plus élevée est élue commutateur de gestion de pile. Vous pouvez attribuer la priorité de gestion. Toutefois, si toutes les unités se voient attribuer la même priorité de gestion, l'unité ayant l'adresse MAC la plus élevée est attribuée comme commutateur de gestion de pile.

Comportement de réinitialisation par défaut de la pile

Si le commutateur de gestion de pile est réinitialisé aux paramètres par défaut définis en usine (voir [Pour rétablir les paramètres par défaut du routeur](#) : à la page 1144), il applique les paramètres par défaut à tous les membres de la pile et réinitialise la pile, y compris tous les membres de la pile participants. Lorsque la pile démarre, le processus de sélection du commutateur de gestion de pile commence.

Limites d'empilement

Une liaison d'empilement fonctionne uniquement sur la vitesse la plus élevée prise en charge par un port de pile. Par exemple, un port 25G qui est également capable de fonctionner à la vitesse 10G fonctionne uniquement à la vitesse 25G en mode pile. Lorsque vous configurez une liaison d'empilement entre deux commutateurs, vous devez vous assurer que les deux ports fonctionnent à la même vitesse. Par exemple,

configurez une liaison d'empilement entre deux ports prenant chacun en charge une vitesse maximale de 25G, ou entre deux ports prenant chacun en charge une vitesse maximale de 10G.

❗ Remarque: En mode Ethernet, cette limitation ne s'applique pas et le port peut fonctionner à 25G ou à une vitesse inférieure.

Les fonctions suivantes ne sont pas compatibles avec l'empilement, vous ne pouvez donc pas les activer sur une pile :

- Precision Time Protocol (Protocole de temps de précision) (voir [Horloge transparente a protocole temporel de PRECISION](#) à la page 136 et [Horloge limite de protocole de temps de précision et horloge grand maître](#) à la page 139)
- Pontage audio/vidéo 802.1AS (voir [802.1AS synchronisation et synchronisation](#) à la page 490)
- Protocole d'enregistrement multiple et 802.1Qav (voir [Protocole d'enregistrement multiple et 802.1Qav](#) à la page 498)

Configurer une pile

Vous pouvez configurer une pile en configurant le commutateur de gestion et en ajoutant un commutateur de gestion de secours et des membres réguliers à la pile. Vous pouvez également définir le mode exemple de pile, qui définit la façon dont les horodatages des messages de pulsation entre les membres de la pile sont calculés, et le mode hachage de jonction de pile, qui définit la façon dont les messages entre les membres de la pile sont sécurisés.

❗ Remarque: Vous pouvez également réaffecter la fonctionnalité de commutateur de gestion de pile d'un commutateur à un autre. Dans ce cas, la configuration de pile entière (y compris toutes les interfaces de la pile) est supprimée et reconfigurée sur le nouveau commutateur de gestion. Une fois le rechargement terminé, toute la gestion de la pile est effectuée sur le nouveau commutateur de gestion. Pour conserver la configuration actuelle lors de la réaffectation de la gestion de la pile à un autre commutateur, enregistrez la configuration actuelle dans la configuration en cours *avant* de réaffecter la gestion de la pile à un autre commutateur. Un déplacement de pile entraîne la perte de toutes les routes et adresses de couche 2 (elles peuvent être réactivées dans la nouvelle configuration de pile).

Définissez le mode d'échantillonnage de la pile

Le mode d'échantillonnage de pile définit comment les horodatages des messages de pulsation entre les membres de la pile sont calculés. Ces messages de pulsation permettent à tous les membres de la pile de rester synchronisés. Le mode d'échantillonnage de la pile et, s'il est configuré, la taille de l'échantillon s'appliquent à tous les membres de la pile.

Pour définir le mode d'échantillonnage de pile :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > empilement > basique > Configuration de la pile**.

La page Configuration de la pile s'affiche. La page affiche différentes sections.

6. Dans la section mode d'échantillonnage pile, dans le menu **mode d'échantillonnage**, sélectionnez le mode :

- **Cumulatif** : Effectue le suivi cumulatif de la somme des décalages d'horodatage reçus.
 - **Historique**. Suit l'historique des horodatages reçus.
7. Si vous sélectionnez **historique** dans le menu **mode échantillon**, dans le champ **nombre max. D'échantillons**, saisissez le nombre maximal d'échantillons à conserver.
La plage est de 100 à 500 secondes.
 8. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
 9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Ajoutez un commutateur comme commutateur de gestion de pile

Lorsque vous configurez une pile, un commutateur doit fonctionner comme commutateur de gestion de pile. Vous pouvez configurer plusieurs commutateurs de gestion. Dans ce cas, le commutateur avec la priorité la plus élevée fonctionne comme commutateur de gestion.

Pour plus d'informations sur la configuration d'autres rôles de commutateur dans une pile, reportez-vous à la section Ajoutez un membre de la pile ou un commutateur de gestion de secours à la page 57.

Si vous modifiez le rôle d'un membre de pile existant en rôle de commutateur de gestion, reportez-vous à la section Modifiez le réglage d'un commutateur dans la pile à la page 60.

Pour ajouter un commutateur en tant que commutateur de gestion de pile :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > empilement > basique > Configuration de la pile**.

La page Configuration de la pile s'affiche. La page affiche différentes sections.

6. Dans le menu **ID unité**, sélectionnez un ID compris entre **1** et **8**.

Il s'agit de l'ID du commutateur de gestion.

7. Dans le menu **type de commutateur**, sélectionnez le modèle de commutateur.

8. Vous pouvez également, dans le menu **priorité du commutateur**, sélectionner la priorité du commutateur qui détermine si et quand le commutateur devient le commutateur de gestion de pile dans le processus de sélection de gestion de pile automatique.

La priorité est en relation avec le réglage de priorité pour les autres commutateurs de la pile. Une valeur plus élevée indique une priorité plus faible. La valeur maximale est 15. La valeur par défaut est non affectée. Si vous définissez la priorité sur zéro, le commutateur ne peut pas devenir un commutateur de gestion de pile. Toutefois, si le commutateur a été affecté ou sélectionné précédemment, informatique reste le commutateur de gestion de la pile et les autres unités sont des membres de la pile.

9. Dans le menu **État de gestion**, sélectionnez **gestion**.

10. Cliquez sur le bouton **Add** (Ajouter).

Vos paramètres sont enregistrés et le commutateur est ajouté à la pile en tant que commutateur de gestion.

11. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la section : Le champ État de veille ne s'applique pas au commutateur de gestion.

Champ	Description
Préférence de gestion du matériel	Préférence de gestion du matériel du commutateur, qui peut être Désactivé ou non attribué.
État de veille	État du commutateur de gestion de veille du commutateur : • CFG Standby : Le commutateur est configuré comme commutateur de gestion de veille. Si le commutateur de gestion de pile actuel tombe en panne, ce commutateur devient le commutateur de gestion de pile. • Veille OPR : Le commutateur fonctionne en tant que commutateur de gestion de secours car le commutateur de gestion de secours configuré a échoué ou n'est plus membre de la pile. • Aucun : Le commutateur n'est pas configuré comme commutateur de gestion de veille.
État du commutateur	L'état du commutateur dans la pile : • OK : Le commutateur est connecté et fonctionne correctement. • Non pris en charge : Le commutateur n'est pas pris en charge. • Non-concordance de code : La version du micrologiciel est différente de celle du commutateur de gestion de pile. • Non-concordance config : Le commutateur ne correspond pas aux commutateurs de la pile. • Absent : Le commutateur n'est pas connecté. • Discordance SDM : Le modèle SDM (Switch Database Management) ne correspond pas. • Mise à jour du code : Une mise à jour du micrologiciel (firmware) est en cours. • Discordance STM : Une incompatibilité du gestionnaire de pile (STM) s'est produite.

Ajoutez un membre de la pile ou un commutateur de gestion de secours

Vous pouvez ajouter un commutateur à une pile et configurer le rôle du commutateur en tant que membre de la pile ou commutateur de secours :

- **Membre de la pile** : Le commutateur est un membre de la pile, mais pas le commutateur de gestion ou un commutateur de secours.
- **Commutateur de gestion de veille** : Le commutateur de gestion de secours prend le relais en tant que commutateur de gestion de pile si celui-ci devient indisponible.

Pour plus d'informations sur l'ajout du commutateur de gestion, reportez-vous à la section [Ajoutez un commutateur comme commutateur de gestion de pile](#) à la page 55.

Pour plus d'informations sur la modification des paramètres d'un commutateur dans la pile, reportez-vous à la section [Modifiez le réglage d'un commutateur dans la pile](#) à la page 60.

Pour ajouter un membre de la pile ou un commutateur de gestion de veille :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > empilement > basique > Configuration de la pile**.

La page Configuration de la pile s'affiche. La page affiche différentes sections.

6. Accédez à la section Configuration de la pile.

Si vous avez déjà ajouté un ou plusieurs commutateurs en tant que membres de la pile, les membres apparaissent dans le tableau.

7. Dans le menu **ID unité**, sélectionnez l'ID du membre.

8. Dans le menu **type de commutateur**, sélectionnez le modèle de commutateur.

9. Vous pouvez également, dans le menu **priorité du commutateur**, sélectionner la priorité du commutateur qui détermine si et quand le commutateur devient le commutateur de gestion de pile dans le processus de sélection de gestion de pile automatique.

La priorité est en relation avec le réglage de priorité pour les autres commutateurs de la pile. Une valeur plus élevée indique une priorité plus faible. La valeur maximale est 15. La valeur par défaut est non affectée. Si vous définissez la priorité sur zéro,

le commutateur ne peut pas devenir un commutateur de gestion de pile. Toutefois, si le commutateur a été affecté ou sélectionné précédemment, informatique reste le commutateur de gestion de la pile et les autres unités sont des membres de la pile.

10. Dans le menu **État de gestion**, indiquez si le commutateur doit fonctionner en tant que membre de la pile (**membre de la pile**) ou en tant que commutateur de gestion de veille (**veille**).

11. Cliquez sur le bouton **Add** (Ajouter).

Les paramètres sont enregistrés. Le commutateur est ajouté en tant que membre de la pile ou en tant que commutateur de secours.

12. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la section :

Champ	Description
Préférence de gestion du matériel	Préférence de gestion du matériel du commutateur, qui peut être Désactivé ou non attribué.
État de veille	État du commutateur de gestion de veille du commutateur : • CFG Standby : Le commutateur est configuré comme commutateur de gestion de veille. Si le commutateur de gestion de pile actuel tombe en panne, ce commutateur prend en charge la gestion de pile. • Veille OPR : Le commutateur fonctionne en tant que commutateur de gestion de secours car le commutateur de gestion de secours configuré a échoué ou n'est plus membre de la pile. • Aucun : Le commutateur n'est pas configuré comme commutateur de gestion de veille.
État du commutateur	L'état du commutateur dans la pile : • OK : Le commutateur est connecté et fonctionne correctement. • Non pris en charge : Le commutateur n'est pas pris en charge. • Non-concordance de code : La version du micrologiciel est différente de celle du commutateur de gestion de pile. • Non-concordance config : Le commutateur ne correspond pas aux commutateurs de la pile. • Absent : Le commutateur n'est pas connecté. • Discordance SDM : Le modèle SDM (Switch Database Management) ne correspond pas. • Mise à jour du code : Une mise à jour du micrologiciel (firmware) est en cours. • Discordance STM : Une incompatibilité du gestionnaire de pile (STM) s'est produite.

Modifiez le réglage d'un commutateur dans la pile

Vous pouvez modifier les paramètres d'un commutateur dans la pile, y compris l'ID d'unité, la priorité par rapport aux autres commutateurs dans la pile et le rôle du commutateur dans la pile.

Pour modifier les paramètres d'un commutateur dans la pile :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > empilement > basique > Configuration de la pile**.

La page Configuration de la pile s'affiche. La page affiche différentes sections.

6. Dans la section Configuration de la pile, cochez la case correspondant à l'ID d'unité du membre de la pile.
7. Pour définir un autre ID pour le membre, dans le champ **changer ID commutateur en**, saisissez un ID.

 **Attention:** Le processus de renumérotation provoque le redémarrage du commutateur après que vous avez cliqué sur le bouton appliquer.

8. Si vous avez précédemment attribué un modèle de commutateur incorrect, sélectionnez le modèle de **commutateur** approprié dans le menu **type de commutateur**.
9. Pour modifier la priorité du commutateur par rapport aux autres commutateurs de la pile, dans le menu **priorité du commutateur**, sélectionnez la priorité du commutateur qui détermine si et quand le commutateur devient le commutateur de gestion de pile.

La priorité est en relation avec le réglage de priorité pour les autres commutateurs de la pile. Une valeur plus élevée indique une priorité plus faible. La valeur maximale est 15. La valeur par défaut est non affectée. Si vous définissez la priorité sur zéro, le commutateur ne peut pas devenir un commutateur de gestion de pile. Toutefois, si le commutateur a été affecté ou sélectionné précédemment, informatique reste le commutateur de gestion de la pile et les autres unités sont des membres de la pile.

10. Pour modifier le rôle du commutateur, dans le menu **État de gestion**, indiquez si le commutateur doit fonctionner en tant que membre de pile normal, commutateur de gestion de pile ou commutateur de gestion de secours :
 - **Membre de la pile** : Le commutateur est un membre de la pile, mais pas le commutateur de gestion ou le commutateur de gestion de secours.
 - **Administration** Le commutateur est le commutateur de gestion de pile.
 - **Veille** Le commutateur est un commutateur de gestion de secours qui prend le relais en tant que commutateur de gestion de pile si celui-ci devient indisponible.

11. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

Si vous définissez un autre ID d'unité pour le commutateur ou modifiez le rôle du commutateur dans la pile, le commutateur redémarre.

12. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Retirez un commutateur de la pile

Vous pouvez supprimer un commutateur qui n'est plus nécessaire dans la pile.

Pour supprimer un commutateur de la pile :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > empilement > basique > Configuration de la pile**.

La page Configuration de la pile s'affiche. La page affiche différentes sections.

6. Dans la section Configuration de la pile, cochez la case correspondant à l'ID d'unité du membre de la pile.
7. Cliquez sur le bouton **Supprimer**.

Vos paramètres sont enregistrés et le commutateur est supprimé de la pile.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez le mode pile pour un port

Par défaut, les ports Ethernet d'un commutateur sont configurés comme ports Ethernet standard pour le trafic Ethernet. Toutefois, vous pouvez configurer un port Ethernet en tant que port de pile pouvant se connecter à un port de pile sur un autre membre de pile.

Pour configurer le mode pile d'un port :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > empilage > Avancé > Configuration des ports de pile** .

La page Stack-port Configuration s'affiche.

6. Pour afficher l'état de la pile d'un commutateur empilé spécifique, sélectionnez l'ID d'unité du commutateur empilé ou sélectionnez le lien **tous** pour afficher l'état de la pile de tous les commutateurs empilés.

Les ports du ou des commutateurs sélectionnés s'affichent.

7. Cochez les cases d'un ou plusieurs ports.

8. Dans le menu **Configured Stack mode**, sélectionnez le mode de fonctionnement du port :

- Stack Le port peut se connecter au port de pile d'un autre commutateur empilé.
- Ethernet : Le port fonctionne comme un port de commutateur Ethernet standard qui reçoit et transmet le trafic réseau. Il s'agit de l'option par défaut.

9. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Champ	Description
ID de l'unité	ID de l'unité pour le commutateur empilé
Port	Port sur le commutateur empilé
Type	Type de port
Nom du produit	Le nom du module émetteur-récepteur à fibre optique installé, le cas échéant
Exécution du mode pile	Mode de fonctionnement du port. Par exemple, vous pouvez configurer un port pour l'empilement, mais jusqu'à ce que vous redémarriez le commutateur, le mode de fonctionnement du port reste le mode Ethernet. Après le redémarrage du commutateur, le mode de fonctionnement passe en mode pile.
Etat de liaison	État de liaison du port. Haut ou bas
Vitesse de liaison (Gbit/s)	Vitesse maximale du port en Gbit/s.
Débit de transmission (Mbit/s)	Débit de transmission approximatif en Mbit/s sur le port
Taux d'erreur de transmission (erreurs/s)	Nombre d'erreurs dans les paquets transmis par seconde
Nombre total d'erreurs de transmission	Nombre total d'erreurs dans les paquets transmis depuis le redémarrage du commutateur. Le compteur peut redémarrer.
Débit de données en réception (Mbit/s)	Débit de réception approximatif en Mbit/s sur le port
Taux d'erreur de réception (erreurs/s)	Nombre d'erreurs dans les paquets reçus par seconde.
Nombre total d'erreurs de réception	Nombre total d'erreurs dans les paquets reçus depuis le redémarrage du commutateur. Le compteur peut redémarrer.
Lier les volets	Nombre total de volets de liaison

Configurer la synchronisation du micrologiciel de pile

Vous pouvez configurer si le micrologiciel de pile est automatiquement synchronisé, si une rétrogradation du micrologiciel vers une version antérieure est autorisée et si des interruptions SNMP sont générées.

Pour configurer la synchronisation du micrologiciel de pile :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > empilement > Avancé > synchronisation du micrologiciel de pile**.

La page synchronisation du micrologiciel de pile s'affiche.

6. Sélectionnez le bouton radio Stack Firmware Auto Upgrade pour spécifier ce qui se passe si vous ajoutez un nouveau membre de la pile et que sa version de micrologiciel ne correspond pas à la version du commutateur de gestion de pile :

- Activer. Le commutateur de gestion de la pile met à jour la version du micrologiciel sur le nouveau membre de la pile afin que l'information corresponde à la version du micrologiciel sur la pile.
 - Désactiver : Le commutateur de gestion de pile ne met pas à jour la version du micrologiciel sur le nouveau membre de pile, ce qui empêche effectivement le nouveau membre de pile de rejoindre la pile.
7. Sélectionnez un bouton radio recouvrements pour spécifier ce qui se passe si vous ajoutez un nouveau membre à la pile :
- Activer. Les interruptions SNMP sont envoyées au démarrage et à la fin d'une synchronisation de microprogramme de pile ou après l'échec de la synchronisation.
 - Désactiver : Aucune interruption SNMP n'est envoyée pendant la synchronisation d'un micrologiciel de pile.
8. Sélectionnez le bouton radio autoriser une rétrogradation pour indiquer si une rétrogradation de version de micrologiciel est autorisée si vous ajoutez un nouveau membre de la pile qui exécute une version de micrologiciel ultérieure à la version de micrologiciel de la pile :
- Activer. Le commutateur de gestion de la pile rétrograde la version du micrologiciel sur le nouveau membre de la pile afin que l'information corresponde à la version du micrologiciel sur la pile.
 - Désactiver : Le commutateur de gestion de pile ne rétrograde pas la version du micrologiciel sur le nouveau membre de pile, ce qui peut effectivement empêcher un commutateur de rejoindre la pile.
9. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez le mode de hachage de la jonction

Le mode de hachage de jonction détermine le mode d'équilibrage de charge utilisé pour une pile. Après avoir sélectionné le mode de hachage de jonction, le commutateur équilibre le trafic en sélectionnant l'une des liaisons sur lesquelles des paquets spécifiques doivent être transmis. Le commutateur sélectionne la liaison en créant un motif binaire à partir de champs sélectionnés dans un paquet et en associant ce motif à une liaison particulière.

Pour configurer le mode de hachage de la jonction :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.
4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **système > empilage > Avancé > Configuration des ports de pile** .
La page Stack-port Configuration s'affiche.
6. Pour afficher l'état de la pile d'un commutateur empilé spécifique, sélectionnez l'ID d'unité du commutateur empilé ou sélectionnez le lien **tous** pour afficher l'état de la pile de tous les commutateurs empilés.
Les ports du ou des commutateurs sélectionnés s'affichent.
7. Cochez la case correspondant à un ou plusieurs ports :
8. Dans le menu **Stack Trunk Hash mode**, sélectionnez le mode :
 - **1 SRC MAC, VLAN, EType, Port entrant** : Adresse MAC source, VLAN, EtherType et port entrant associés au paquet
 - **2 Dest MAC, VLAN, EType, Port entrant** : Adresse MAC de destination, VLAN, EtherType et port entrant associés au paquet
 - **3 SRC/destination MAC, VLAN, EType, Port entrant** : Adresses MAC source et de destination, VLAN, EtherType et port entrant associés au paquet

- **4 champs SRC IP et SRC TCP/UDP Port** : Champs adresse IP source et port TCP/UDP source du paquet
 - **5 champs adresse IP destination et Port TCP/UDP destination** : Champs adresse IP de destination et port TCP/UDP de destination du paquet
 - **6 champs SRC/Dest IP et TCP/UDP Port** : Les adresses IP source et de destination et les champs de port TCP/UDP source et de destination du paquet.
 - **7 mode de hachage amélioré** : Sélections dynamiques de champs basées sur le flux de paquets. Pour les paquets L2, les adresses MAC source et de destination sont utilisées ; pour les paquets IP, les adresses IP source et de destination et les champs de port TCP/UDP sont utilisés.
9. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Affiche des informations sur la configuration de la pile

Vous pouvez afficher des informations sur la configuration de la pile.

Pour afficher des informations sur la configuration de la pile :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > empilement > basique > Configuration de la pile**.

La page Configuration de la pile s'affiche. La page affiche différentes sections.

6. Accédez à la section État de la pile de base.

Le tableau suivant décrit les champs en lecture seule de la section :

Champ	Description
ID de l'unité	ID d'unité du commutateur dans la pile
Description du commutateur	La description du commutateur, qui est effectivement le numéro de modèle du commutateur
Numéro de série	Le numéro de série du contacteur
Durée de fonctionnement	Période écoulée depuis le redémarrage du commutateur
Identificateur de modèle préconfiguré	Le type de modèle attribué par le fabricant du commutateur, qui est effectivement le numéro de modèle du commutateur
Identificateur de modèle branché	Type de modèle attribué par le fabricant du commutateur pour identifier le commutateur branché. (L'identificateur de modèle connecté peut être identique à l'identificateur de modèle préconfiguré.)
Version de code détectée	Version détectée du micrologiciel du commutateur
Code détecté dans Flash	Version détectée du micrologiciel du commutateur dans la mémoire flash
État de la dernière tentative SFS	État de la synchronisation du micrologiciel de pile (SFS) la plus récente.

Affiche l'état de la pile de messages de pulsation

Vous pouvez afficher l'état de la pile de messages de pulsation et effacer les informations d'échantillonnage. Un message de pulsation est un message qu'un commutateur empilé échange avec ses voisins.

Pour afficher l'état de la pile de messages de pulsation et effacer les informations d'échantillonnage :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > empilement > Avancé > État de la pile**.

La page État de la pile s'affiche.

6. Pour afficher l'état de la pile d'un commutateur empilé spécifique, sélectionnez l'ID d'unité du commutateur empilé ou sélectionnez le lien **tous** pour afficher l'état de la pile de tous les commutateurs empilés.

Le tableau suivant décrit les champs en lecture seule de la section :

Champ	Description
ID de l'unité	ID d'unité du commutateur dans la pile
ID de l'unité voisine	ID de l'unité voisine avec laquelle les données sont échangées
Actuel	Heure actuelle de réception du message de pulsation
Moyenne	Temps moyen entre deux messages de pulsation entrants consécutifs
Min	Temps minimum entre deux messages de pulsation entrants consécutifs
Max	Temps maximum entre deux messages de pulsation entrants consécutifs
Abandonné	Nombre de messages de pulsation perdus ou abandonnés

7. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).
8. Pour effacer les informations d'échantillonnage, procédez comme suit :
 - a. Dans le menu **Effacer compteurs**, sélectionnez un ID d'unité ou sélectionnez **tous**.
 - b. Cliquez sur le bouton **Apply** (Appliquer).
Les compteurs sont effacés.
9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Affiche les informations de diagnostic, d'état et de chemin du port de pile

Les diagnostics de port de pile vous permettent d'afficher les informations de diagnostic, d'état et de chemin d'accès d'un port de pile.

Pour exécuter les diagnostics de port de pile :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > empilement > Avancé > Diagnostics de port de pile**.

La page Diagnostics Stack-port s'affiche.

6. Dans la section Diagnostics de port de pile, pour afficher les informations de diagnostic d'un commutateur empilé spécifique, sélectionnez l'ID d'unité du commutateur empilé ou sélectionnez le lien **tous** pour afficher les informations de diagnostic de tous les commutateurs empilés.

Les ports du ou des commutateurs sélectionnés s'affichent.

Pour chaque port de pile, le champ Port Diagnostics Info affiche des informations de diagnostic et d'état.

7. Dans la section Stack-port packet-path, pour afficher des informations sur le chemin des paquets entre les ports de pile, sélectionnez l'ID d'unité du commutateur empilé ou sélectionnez la liaison **All** pour afficher les informations de diagnostic de tous les commutateurs empilés.

Le champ Direction affiche le numéro d'unité de pile à partir duquel le chemin de pile est calculé.

Le champ chemin-paquet affiche le numéro de port de pile (par exemple, 2/0/28) connecté à l'unité de pile à partir de laquelle le chemin de pile est calculé.

8. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).
9. Pour effacer les statistiques, cliquez sur le bouton **Effacer**.
10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Retirez une pile

Vous pouvez supprimer une pile en supprimant tous les commutateurs de la pile.

Pour supprimer une pile :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.
4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **système > empilement > basique > Configuration de la pile** .
La page Configuration de la pile s'affiche. La page affiche différentes sections.
6. Dans la section Configuration de la pile, cochez toutes les cases des unités de la pile.
Vous ne pouvez pas supprimer le commutateur de gestion de pile.
7. Cliquez sur le bouton **Supprimer**.
Vos paramètres sont enregistrés et les unités sont supprimées de la pile.
8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Transfert continu de pile

Le transfert NSF (NonStop Forward) permet au plan de transfert des membres de la pile de continuer à transférer des paquets pendant que les plans de contrôle et de gestion redémarrent à la suite d'une panne de courant, d'une panne matérielle ou d'une panne logicielle sur le commutateur de gestion. Si le commutateur de gestion tombe en panne, les flux de trafic peuvent continuer à entrer et sortir de la pile via les ports physiques de tout membre autre que le commutateur de gestion avec moins d'une seconde d'interruption.

Vous pouvez également lancer un basculement de transfert continu vers un commutateur de gestion de secours (voir [Configurer le transfert continu et afficher les informations associées](#) à la page 75).

Pour préparer le commutateur de gestion de secours, les applications du commutateur de gestion transmettent en continu des informations à l'unité de secours. Les modifications apportées à la configuration en cours sont automatiquement copiées sur le commutateur de gestion de secours. Les adresses MAC restent les mêmes lors d'un basculement de transfert non-stop afin que les voisins ne soient pas tenus de les réapprendre.

Lorsqu'un basculement de transfert ininterrompu se produit, le plan de contrôle sur le commutateur de gestion de secours applique les informations que l'ordinateur a reçues du commutateur de gestion. Lorsque le plan de contrôle est en cours d'initialisation, la pile ne peut pas réagir aux modifications externes, telles que les modifications de topologie du réseau. Une fois que le plan de contrôle est entièrement opérationnel sur le nouveau commutateur de gestion (qui était auparavant le commutateur de gestion de secours), le plan de contrôle met à jour les modifications matérielles nécessaires. Le temps de basculement du plan de contrôle dépend de la taille de la pile, de la complexité de la configuration et de la vitesse du CPU du commutateur.

Le plan de gestion redémarre lorsqu'un basculement se produit. Les connexions de gestion doivent être rétablies.

Pour que NSF soit efficace, les périphériques réseau adjacents ne doivent pas réacheminer le trafic autour du périphérique de redémarrage. Le commutateur utilise trois techniques pour empêcher le reroutage du trafic :

- Un protocole peut distribuer une partie de son plan de contrôle aux membres de la pile afin que le protocole puisse donner l'impression que l'ordinateur est toujours

fonctionnel pendant le redémarrage. Le Spanning Tree et les canaux de port utilisent cette technique.

- Un protocole peut obtenir la coopération de ses voisins par une technique connue sous le nom de redémarrage gracieux. OSPF (voir [Configurez OSPF et OSPFv3](#) à la page 606) utilise le redémarrage progressif si vous activez cette option.
- Un protocole peut redémarrer après le basculement si les voisins réagissent suffisamment lentement pour ne pas détecter la panne. Les protocoles de routage multicast IP sont un bon exemple de ce comportement.

Pour tirer pleinement parti du transfert ininterrompu, les connexions de couche 2 aux voisins doivent passer par des canaux de port qui couvrent au moins deux membres de la pile, et les routes de couche 3 doivent être des routes ECMP (Equal Cost Multipath) avec des sauts suivants via des ports physiques sur au moins deux membres de la pile. Le matériel peut rapidement déplacer les flux de trafic des membres du canal de port ou des chemins ECMP sur une unité défaillante vers une unité survivante.

Configurer le transfert continu et afficher les informations associées

Le transfert NSF (NonStop Forward) permet à un commutateur de gestion de secours de prendre le relais si le commutateur de gestion de pile tombe en panne ou devient indisponible.

Pour configurer le transfert continu et afficher les informations associées :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > empilement > Avancé > Résumé NSF**.

La page Récapitulatif NSF s'affiche.

6. Sélectionnez un bouton radio Statut administrateur :

- Désactiver : NSF est désactivé.
- Activer. NSF est activé. Il s'agit de l'option par défaut. Lorsque NSF est activé, la pile sélectionne automatiquement un commutateur de gestion de secours en fonction des paramètres des membres de la pile (voir [Ajoutez un membre de la pile ou un commutateur de gestion de secours](#) à la page 57). Le commutateur de gestion de pile copie les informations de pile vers le commutateur de gestion de secours.

7. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

9. Pour lancer manuellement une commutation NSF du commutateur de gestion de pile au commutateur de gestion de secours, cliquez sur le bouton **Initiate Failover**.

Le commutateur de gestion de secours devient le commutateur de gestion de pile.

Le tableau suivant décrit les champs en lecture seule de la page.

Champ	Description
Section Résumé NSF	
Statut opérationnel	Indique si NSF est activé sur le commutateur de gestion de secours

(A continué)

Champ	Description
Motif du dernier démarrage	La raison du passage le plus récent à NSF : • Allumé Le commutateur de gestion de pile a redémarré, par exemple en raison d'un cycle d'alimentation ou de l'exécution d'une commande de rechargement, et le commutateur de gestion de secours a pris le relais. • Déplacement admin à froid : Le commutateur de gestion de pile réinitialise toutes les informations sans redémarrer réellement, le commutateur de gestion de secours a pris le relais et a commencé à partir d'un état préinitialisé, et aucune donnée n'est conservée avant le basculement. • Déplacement de l'administrateur chaud : Vous avez appuyé sur le bouton Initiate Failover ou sur une commande CLI pour que le commutateur de gestion de secours prenne le relais. • Préchauffage automatique : Le commutateur de gestion de pile a redémarré en raison d'une panne et le commutateur de gestion de secours a pris le relais. • Auto froid : Le commutateur de gestion de secours a pris le relais et le trafic de données utilisateur a été interrompu. Cette situation peut être causée par plusieurs défaillances se produisant à proximité.
Temps écoulé depuis le dernier redémarrage	Période depuis que le commutateur de gestion actuel est devenu le commutateur de gestion actif. Pour le commutateur de gestion de veille, la valeur est définie sur 0.
Redémarrage en cours	Indique si un basculement du commutateur de gestion de pile vers le commutateur de gestion de secours est en cours. Un redémarrage n'est pas considéré comme terminé tant que toutes les informations ne sont pas complètement rapprochées.
Redémarrage à chaud prêt	Le commutateur de gestion de pile est synchronisé avec le commutateur de gestion de secours, et le commutateur de gestion de pile peut être redémarré, si nécessaire.
Copie de la configuration en cours vers l'unité de sauvegarde	
Etat	État de la copie de la configuration en cours sur le commutateur de gestion de secours
Temps écoulé depuis la dernière copie	Période écoulée depuis que la configuration en cours a été copiée sur le commutateur de gestion de secours
Prise en charge NSF sur l'unité	
ID de l'unité	ID d'unité du commutateur dans la pile
Prise en charge du NSF	Indique si le commutateur de la pile est capable de prendre en charge NSF

Afficher les statistiques de point de contrôle de transfert ininterrompu

Les statistiques de point de contrôle sont les statistiques des messages automatisés envoyés entre le commutateur de gestion et le commutateur de gestion de secours.

Pour afficher les statistiques de point de contrôle de transfert ininterrompu :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > empilement > basique > statistiques de point de contrôle**.

La page Checkpoint Statistics s'affiche.

6. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

7. Pour effacer les statistiques, cliquez sur le bouton **Effacer**.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Champ	Description
Point de contrôle des messages	Nombre de messages envoyés du commutateur de gestion de pile au commutateur de gestion de secours
Octets avec point de contrôle	Quantité de données en octets envoyée du commutateur de gestion de pile au commutateur de gestion de secours

(A continué)

Champ	Description
Temps écoulé depuis l'effacement des compteurs	Période écoulée depuis la réinitialisation des compteurs
Taux de messages de point de contrôle	Nombre de secondes ou fractions de secondes entre les mesures
Taux de messages des 10 dernières secondes	Nombre de messages envoyés au cours du dernier intervalle de mesure de 10 secondes
Taux de messages de 10 secondes le plus élevé	Le plus grand nombre de messages envoyés dans un intervalle de mesure de 10 secondes

3

Configurer les informations système du commutateur

Ce chapitre aborde les sujets suivants :

- [Informations sur le système et le logement du commutateur](#)
- [Interfaces de bouclage](#)
- [Interfaces de gestion IPv4 et VLAN](#)
- [Interfaces de gestion IPv6 et VLAN](#)
- [Paramètres heure et NTP](#)
- [Horloge transparente a protocole temporel de PRECISION](#)
- [Horloge limite de protocole de temps de précision et horloge grand maître](#)
- [Système de noms de domaine](#)
- [Changer de modèle de gestion de base de données](#)
- [Paramètres Ethernet verts](#)
- [Paramètres Bonjour](#)
- [Activer ou désactiver la capacité du serveur TFTP](#)
- [Serveur DHCP IPv4](#)
- [Relais DHCP](#)
- [Relais DHCP de couche 2](#)
- [Relais UDP](#)
- [Serveur DHCPv6](#)
- [Interface de relais DHCPv6](#)
- [Power over Ethernet](#)

- Programmations de minuterie
- Simple Network Management Protocol
- LLDP (Link Layer Discovery Protocol)
- Protocole de découverte de couche de liaison pour les périphériques de point d'extrémité multimédia
- Dépendance de liens
- Protocole de découverte standard de l'industrie

Informations sur le système et le logement du commutateur

Vous pouvez configurer la vue et configurer les informations système du commutateur.

Afficher et configurer les informations système du commutateur

Lorsque vous vous connectez, la page informations système s'affiche. Vous pouvez configurer et afficher des informations générales sur le périphérique.

Pour afficher et définir les informations système :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Définissez les champs suivants :

- **Nom du système** : Entrez le nom pour identifier ce commutateur. Vous pouvez utiliser jusqu'à 255 caractères alphanumériques. La valeur par défaut est vide.
- **Emplacement du système** : Entrez l'emplacement de ce commutateur. Vous pouvez utiliser jusqu'à 255 caractères alphanumériques. La valeur par défaut est vide.
- **Contact système** : Saisissez la personne à contacter pour ce commutateur. Vous pouvez utiliser jusqu'à 255 caractères alphanumériques. La valeur par défaut est vide.
- **Délai de connexion** : Spécifiez le nombre de minutes d'inactivité pouvant survenir sur une connexion de port série avant que le commutateur ne ferme la connexion. Saisissez une valeur comprise entre 0 et 160. La valeur par défaut est 5. La saisie de 0 désactive le délai d'attente.
- **Interface de la source de gestion** : Sélectionnez l'interface de gestion à utiliser comme interface source pour les fonctions SNMP trap, syslog, DNS, TACACS+, RADIUS, sFlow et NTP. Par défaut, les options suivantes s'affichent dans le menu :
 - Aucun : L'adresse IP principale de l'interface d'origine (sortante) est utilisée comme adresse source.
 - VLAN 1 L'adresse IP principale de VLAN 1 est utilisée comme adresse source. Il s'agit de la sélection par défaut.
 - Port de service L'adresse IP du port de gestion est utilisée comme adresse source.

Selon la configuration de votre commutateur, les options suivantes peuvent s'afficher :

- **Un autre identifiant VLAN** : L'adresse IP principale d'un VLAN autre que VLAN 1 est utilisée comme adresse source.
- **Interface de routage** : L'adresse IP principale d'une interface de routage est utilisée comme adresse source.
- VLAN de routage L'adresse IP principale d'une interface de routage VLAN est utilisée comme adresse source.
- **Interface de bouclage de routage** : L'adresse IP principale d'une interface de bouclage de routage est utilisée comme adresse source.
- **Différent**: Applications pour lesquelles l'interface source est configurée séparément.

6. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

7. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les informations d'état dans les sections informations sur l'application et informations sur le système de la page.

Table 6 : Informations sur l'application et informations sur le système

Champ	Description
Informations sur l'application	
Nom de l'application	Nom de l'application qui s'exécute sur le commutateur. AVUI, ConfigAgent et discAgent sont des exemples d'applications pouvant être en cours d'exécution.
État de l'application	État de l'application
Version	Version de l'application
Informations système	
Nom du produit	Le nom du produit (nom du modèle) de ce commutateur
Adresse de gestion IPv4	Adresse IPv4 et masque attribués à l'interface VLAN de gestion
Adresse de gestion IPv6	Adresse IPv6 et masque attribués à l'interface VLAN de gestion
Interface de gestion IPv4	ID VLAN de gestion IPv4 du commutateur. Cliquez sur la valeur de l'ID VLAN de gestion affichée pour passer à la page de configuration. Consultez la section Configurez un VLAN de gestion IPv4 à la page 102.
Interface de gestion IPv6	ID VLAN de gestion IPv6 du commutateur. Cliquez sur la valeur de l'ID VLAN de gestion affichée pour passer à la page de configuration. Consultez la section Configurez un VLAN de gestion IPv6 à la page 110.
Interface de bouclage IPv4	Adresse IPv4 et masque attribués à l'interface de bouclage
Interface de bouclage IPv6	Préfixe IPv6 et longueur de préfixe affectés à l'interface de bouclage
Date système	Date actuelle
OID SNMP du système	ID d'objet de base pour la MIB d'entreprise de commutateur
Adresse MAC du système	Adresse réseau MAC attribuée universellement

Afficher l'état du ventilateur

Cette page affiche l'état des ventilateurs de toutes les unités. Ces ventilateurs éliminent la chaleur générée pendant le fonctionnement par les ports d'alimentation PoE (pour les modèles prenant en charge PoE), le processeur et d'autres composants internes, pour permettre aux chipsets de fonctionner normalement.

L'état du ventilateur peut être l'un des suivants :

- Fonctionnement : Le ventilateur fonctionne normalement.
- Echec Le ventilateur est défectueux.

- **Absent** : Le ventilateur est absent. (Le nombre de ventilateurs dépend du modèle de commutateur.)
- **Stop** (Arrêter) - Le ventilateur s'est arrêté car la température de fonctionnement est basse. Le ventilateur démarre si la température de fonctionnement dépasse un seuil prédéfini.

Pour afficher l'état du ventilateur :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Faites défiler jusqu'à la section État du ventilateur.

6. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

Le tableau suivant décrit les champs d'état du ventilateur en lecture seule. Le tableau peut indiquer l'état du ventilateur pour un maximum de huit commutateurs empilés. Le nombre de ventilateurs dépend du modèle de commutateur.

Table 7 : Informations sur l'état du ventilateur

Champ	Description
ID de l'unité	ID de l'unité du commutateur dans lequel le ventilateur est installé.
Ventilateurs	Le numéro du ventilateur
Description	La description du ventilateur, telle que FAN-1, FAN-2, etc.
Type	Le type de ventilateur, qui est toujours fixe.
Vitesse	La vitesse du ventilateur. Pour plus d'informations, reportez-vous au manuel de l'utilisateur, que vous pouvez télécharger en vous rendant sur le site www.netgear.fr/support/download .
Niveau de service	Niveau de service du ventilateur en pourcentage.
Etat FAN	L'état du ventilateur : • Fonctionnement : Le ventilateur fonctionne normalement. • Echec Le ventilateur est défectueux. • Absent : Le ventilateur n'est pas absent. (Le nombre de ventilateurs dépend du modèle de commutateur.) • Stop (Arrêter) - Le ventilateur s'est arrêté car la température de fonctionnement est basse. Le ventilateur démarre si la température de fonctionnement dépasse un seuil prédéfini.

Afficher les informations du capteur de température

Vous pouvez afficher la température actuelle des différents capteurs du système à l'aide du tableau État de la température.

Pour afficher les informations de température :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Faites défiler jusqu'à la section Etat de la température.

6. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

Le tableau suivant décrit les champs d'état de la température en lecture seule.

Table 8 : Informations sur l'état de la température

Champ	Description
ID de l'unité	ID de l'unité du commutateur dans lequel le capteur est installé.
Capteurs	ID du capteur.
Description	Description du capteur.
Température (C)	La température du capteur en degrés Celsius.
Etat	L'état du capteur, qui doit être normal.
Temp max (C)	Température de fonctionnement maximale prise en charge en degrés Celsius.

Afficher l'état du périphérique et la version du micrologiciel

Vous pouvez afficher l'état du périphérique et la version du micrologiciel.

Pour afficher l'état du périphérique et la version du micrologiciel :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Faites défiler jusqu'à la section Etat de la température.

6. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

Le tableau suivant décrit les champs d'état du périphérique en lecture seule. Le tableau peut afficher l'état du périphérique pour un maximum de huit commutateurs empilés.

Table 9 : Informations sur l'état du périphérique

Champ	Description
ID de l'unité	ID de l'unité du commutateur pour lequel l'état du périphérique s'affiche.
Version du micrologiciel (firmware)	Version, version et numéro de maintenance du micrologiciel exécuté sur le commutateur. Par exemple, si la version est 1, la version est 2 et le numéro de maintenance est 4, le format est 1,2.4.
Version de démarrage	Version du code de démarrage qui se trouve dans la mémoire flash. Le code de démarrage permet de charger le micrologiciel dans la mémoire.
Numéro de série	Le numéro de série du contacteur.

Table 9 : Informations sur l'état du périphérique (A continué)

Champ	Description
PS-1	L'état de l'alimentation interne : • Fonctionnement : Le bloc d'alimentation est présent et fonctionne correctement. • Alimentation. L'alimentation principale a échoué ou le câble d'alimentation est déconnecté mais une alimentation redondante fournit l'alimentation. • Absent : Aucun bloc d'alimentation n'est présent dans le logement. • Non alimenté: Le bloc d'alimentation est présent mais n'est pas connecté à une source d'alimentation. • Pas d'alimentation: L'alimentation est présente et connectée, mais le commutateur utilise une autre source d'alimentation. • Incompatible: L'alimentation est présente mais incompatible. • Echec : Le bloc d'alimentation est présent mais le câble d'alimentation n'est pas branché ou un câble défectueux est branché. • N/A Le commutateur ne prend pas en charge l'alimentation.
Pour les modèles PoE uniquement : MAX PoE	Pour les modèles PoE uniquement : L'état du système PoE sur le commutateur : • Activé. Moins de 10 W de puissance PoE est disponible pour un autre PD. • Eteint. Au moins 10 W de puissance PoE disponible pour un autre PD. • N/A PoE n'est pas pris en charge par le commutateur.
Durée de fonctionnement du système	Temps en jours, heures et minutes depuis le redémarrage du commutateur.

Afficher l'état de l'UC du système

Pour afficher l'état de l'UC du système :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > gestion > État de l'UC du système**.

La page System CPU Status s'affiche.

6. Si vous avez configuré une pile de commutateurs, dans le menu **No unité**, sélectionnez l'ID de l'unité du commutateur dans la pile.

L'état de la mémoire CPU comprend la mémoire totale du commutateur en Ko et l'espace mémoire disponible pour le commutateur en Ko.

L'utilisation du CPU montre l'utilisation du CPU par les différents processus sur le commutateur.

Configurez les seuils de CPU

Vous pouvez configurer des seuils CPU qui déclenchent une notification s'ils sont dépassés. La notification s'effectue par le biais de messages SNMP trap et syslog.

Pour configurer les seuils de CPU :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > gestion > État de l'UC du système > seuil de l'UC**.

La page seuil CPU s'affiche.

6. Configurez les paramètres de seuil UC suivants :

- **Seuil croissant** : Configurez la valeur du seuil d'augmentation. Une notification est générée lorsque l'utilisation totale du CPU dépasse cette valeur de seuil sur la période configurée. La plage est un pourcentage de 1 à 100.
- **Intervalle de montée** : Configurez la valeur de l'intervalle d'augmentation. Configurez cette période de surveillance de l'utilisation de 5 à 86400 secondes par multiples de 5 secondes.
- **Seuil descendant** : Configurez le seuil de chute. Une notification est déclenchée lorsque l'utilisation totale du CPU tombe en dessous de ce niveau pendant une période configurée.
Le seuil d'utilisation décroissant doit être inférieur ou égal à la valeur du seuil croissant. La notification de seuil d'utilisation décroissant n'est générée que si une notification de seuil croissant a été générée précédemment. La configuration du seuil et de la période d'utilisation décroissante est facultative. Si les valeurs d'utilisation du CPU décroissantes ne sont pas configurées, elles prennent la même valeur que les valeurs d'utilisation du CPU croissantes. La plage est un pourcentage de 1 à 100.
- **Intervalle de chute** : Configurez l'intervalle de chute. Vous pouvez configurer la période de surveillance de l'utilisation de 5 secondes à 86400 secondes par multiples de 5 secondes.
- **Seuil de mémoire libre** : Configurez la valeur du seuil de mémoire libre de l'UC en Ko.

7. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Afficher ou effacer les statistiques du commutateur

Pour afficher ou effacer les statistiques du commutateur :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > gestion > statistiques du commutateur**.

La page Switch Statistics s'affiche.

6. Pour effacer tous les compteurs, réinitialiser tous les récapitulatifs des commutateurs et les statistiques détaillées sur les valeurs par défaut, cliquez sur le bouton Effacer.

Le nombre de paquets supprimés ne peut pas être effacé.

7. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les informations statistiques du commutateur.

Table 10 : Informations statistiques du commutateur

Champ	Description
IfIndex	IfIndex de l'entrée de la table d'interface associée au processeur de ce commutateur.
Octets reçus	Nombre total d'octets de données reçus par le processeur (à l'exclusion des bits de trame mais incluant les octets FCS).
Paquets reçus sans erreur	Nombre total de paquets (y compris les paquets de diffusion et les paquets de multidiffusion) reçus par le processeur.
Paquets unicast reçus	Nombre de paquets unicast de sous-réseau livrés à un protocole de couche supérieure.
Paquets multidiffusion reçus	Nombre total de paquets reçus qui ont été dirigés vers une adresse de multidiffusion. Ce nombre n'inclut pas les paquets dirigés vers l'adresse de diffusion.
Paquets de diffusion reçus	Nombre total de paquets reçus qui ont été dirigés vers l'adresse de diffusion. Cela n'inclut pas les paquets multicast.
Réception des paquets ignorés	Nombre de paquets entrants qui ont été rejetés même si aucune erreur n'a été détectée pour empêcher leur livraison à un protocole de couche supérieure. Une raison possible pour rejeter un paquet peut être de libérer de l'espace tampon.
Octets transmis	Nombre total d'octets transmis depuis l'interface, caractères de tramage compris.
Paquets transmis sans erreurs	Nombre total de paquets transmis depuis l'interface.
Paquets unicast transmis	Nombre total de paquets que les protocoles de niveau supérieur ont demandés et qui sont transmis à une adresse de monodiffusion de sous-réseau, y compris ceux qui ont été rejetés ou non envoyés.
Paquets multicast transmis	Nombre total de paquets que les protocoles de niveau supérieur ont demandés et qui sont transmis à une adresse de multidiffusion, y compris ceux qui ont été rejetés ou qui n'ont pas été envoyés.
Paquets de diffusion transmis	Nombre total de paquets que les protocoles de niveau supérieur ont demandés et qui sont transmis à l'adresse de diffusion, y compris ceux qui ont été rejetés ou qui n'ont pas été envoyés.
Paquets de transmission ignorés	Nombre de paquets sortants qui ont été rejetés même si aucune erreur n'a été détectée pour empêcher leur livraison à un protocole de couche supérieure. Une raison possible pour rejeter un paquet peut être de libérer de l'espace tampon.
La plupart des entrées d'adresse jamais utilisées	Le plus grand nombre d'entrées de la table d'adresses de la base de données de transfert apprises par ce commutateur depuis le dernier redémarrage.

Table 10 : Informations statistiques du commutateur (A continué)

Champ	Description
Entrées d'adresse en cours d'utilisation	Nombre d'entrées apprises et statiques dans la table d'adresses de la base de données de transfert pour ce commutateur.
Nombre maximum d'entrées VLAN	Nombre maximal de réseaux locaux virtuels (VLAN) autorisés sur ce commutateur.
La plupart des entrées VLAN jamais utilisées	Le plus grand nombre de VLAN actifs sur ce commutateur depuis le dernier redémarrage.
Entrées VLAN statiques	Nombre d'entrées VLAN actuellement actives sur ce commutateur qui ont été créées de manière statique.
Entrées VLAN dynamiques	Nombre d'entrées VLAN actuellement actives sur ce commutateur qui ont été créées par enregistrement GVRP.
Suppression de VLAN	Nombre de VLAN sur ce commutateur qui ont été créés puis supprimés depuis le dernier redémarrage.
Temps écoulé depuis le dernier effacement des compteurs	Temps écoulé, en jours, heures, minutes et secondes, depuis la dernière effacement des statistiques de ce commutateur.

Afficher les informations sur le périphérique USB

Pour afficher les informations sur le périphérique USB :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > gestion > informations sur le périphérique USB**.

La page informations sur le périphérique USB s'affiche.

Le champ Etat du périphérique affiche l'état actuel du périphérique. L'état est l'un des suivants :

- **Actif**. L'appareil est branché et reconnu par le commutateur.
- **Inactif** : L'appareil n'est pas monté.
- **Non valide** Le périphérique n'est pas présent ou un périphérique non valide est branché.

6. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

Le tableau suivant décrit les informations de la section statistiques de la mémoire USB.

Table 11 : Informations statistiques sur la mémoire USB

Champ	Description
Taille totale	Taille de stockage du périphérique flash USB en octets.
Octets utilisés	Taille de la mémoire utilisée sur le périphérique flash USB.
Octets libres	La taille de la mémoire disponible sur le périphérique flash USB.

Le tableau suivant décrit les informations de la section Détails du répertoire USB.

Table 12 : Informations détaillées sur le répertoire USB

Champ	Description
Nom du fichier	Nom du fichier stocké sur la clé USB.
Taille du fichier	Taille du fichier stocké dans la clé USB en octets
Heure de modification	Heure de la dernière modification du fichier stocké sur la clé USB.

Affiche des informations sur une pile et les modèles de commutateur optionnels pour une pile

Vous pouvez afficher des informations sur une pile existante de commutateurs de la série M4350 et les modèles de commutateurs optionnels compatibles avec une pile de commutateurs de la série M4350. Bien que la page suggère que les informations sont pour une configuration d'emplacement, informatique est vraiment pour une configuration de pile de commutateurs.

Pour afficher des informations sur une pile et les modèles de commutateur optionnels pour une pile :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > gestion > informations sur les emplacements**.

La page informations sur le logement s'affiche. La page affiche différentes sections.

6. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

Le tableau suivant décrit les champs en lecture seule du tableau Configuration des emplacements.

Table 13 : Informations sur la configuration des logements (configuration des commutateurs empilés)

Champ	Description
Logement	Le numéro de l'unité et du logement. Cette entrée représente un commutateur empilé. Le premier commutateur est 1/0, le deuxième commutateur est 2/0, le troisième commutateur est 3/0, et ainsi de suite.
Etat	Indique si le commutateur est configuré pour l'empilage (« plein ») ou préconfiguré pour l'empilage (« vide »)
État administratif	L'état administratif est toujours activé
Etat de l'alimentation	L'état d'alimentation est toujours activé
ID de modèle de carte configuré	Le modèle du commutateur de la série M4350
Description de la carte configurée	Description du commutateur série M4350
ID du modèle de carte inséré	Ce champ est identique au champ ID de modèle de carte configuré
Description de la carte insérée	Ce champ est identique au champ Description de la carte insérée
Mise hors tension de la carte	Indique si l'état de l'alimentation peut être activé ou désactivé administrativement. Ce champ est toujours faux.
Carte enfichable	Indique si le commutateur est enfichable. Ce champ est toujours faux.

Le tableau suivant décrit les champs en lecture seule de la table cartes prises en charge.

Table 14 : Informations sur les cartes prises en charge (informations sur les commutateurs de la série M4350 pris en charge pour une pile)

Champ	Description
Modèle de carte	ID de modèle du commutateur pris en charge
Index de carte	Index attribué au commutateur pris en charge
Type de carte	Type de matériel du commutateur pris en charge, attribué par le fabricant
Descripteur de carte	Description du commutateur pris en charge

Le tableau suivant décrit les champs en lecture seule de la table Switch pris en charge. Si vous préconfigurez un nouveau membre de la pile, l'index de commutateur identifie le type de commutateur ajouté à la pile.

Table 15 : Informations sur les commutateurs pris en charge (index des commutateurs et informations sur les préférences de gestion)

Champ	Description
Modèle du switch	Numéro de modèle du commutateur pris en charge
Changer d'index	Index affecté au commutateur pris en charge
Gérer les préférences	Préférence de gestion du commutateur pris en charge

Interfaces de bouclage

Une interface de bouclage vous permet d'envoyer un ping, un traceroute et d'autres trafics de test ainsi que du trafic de protocole au commutateur. Une interface de bouclage nécessite une adresse réseau IPv4 ou IPv6 unique. Vous pouvez ajouter une ou plusieurs interfaces de bouclage.

Pour ajouter une interface de bouclage :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **système > gestion > interface de bouclage** .
La page interface de bouclage s'affiche.
6. Dans le menu **type d'interface de bouclage**, sélectionnez IPv4 ou IPv6.
7. Dans le menu **ID de boucle**, sélectionnez un ID d'interface.
8. Configurez les paramètres suivants, en fonction du type d'interface de bouclage :
 - IPv4 : Pour une interface IPv4, configurez les paramètres suivants :
 - **Adresse IP principale** : Saisissez l'adresse IPv4 principale de cette interface en notation décimale à points.
 - **Masque de sous-réseau IP principal** : Entrez le masque de sous-réseau IPv4 principal en notation décimale à points.
 - IPv6 : Pour une interface IPv6, configurez les paramètres suivants :
 - **Mode IPv6**. Sélectionnez **Activer** pour utiliser l'adresse IPv6 après avoir spécifié informatique. Vous pouvez sélectionner cette option uniquement avant de spécifier l'adresse IPv6.
 - Préfixe IPv6 Saisissez le préfixe IPv6.
 - Longueur de préfixe : Entrez la longueur du préfixe IPv6.
 - EUI64 : Activez ou désactivez l'identificateur unique étendu 64 bits (EUI-64).
9. Cliquez sur le bouton **Add** (Ajouter).
Vos paramètres sont enregistrés et l'interface de bouclage est ajoutée.
Les champs État de l'interface de bouclage indiquent si l'interface de bouclage est active.
10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Interfaces de gestion IPv4 et VLAN

L'interface utilisateur principale fournit des options de configuration IPv4 que vous pouvez utiliser pour configurer la gestion IP basée sur VLAN ou basée sur les ports.

Par défaut, l'interface source des applications est VLAN 1. Si vous modifiez les valeurs VLAN et port de gestion IPv4, l'interface source passe également automatiquement aux valeurs VLAN et port par défaut VLAN 1.

Vous pouvez accéder au commutateur sur l'interface utilisateur principale par l'une des méthodes suivantes :

- **Port de service IPv4** : Le port de service est un port Ethernet dédié pour la gestion hors bande du commutateur. Le trafic de gestion sur ce port est séparé du trafic réseau opérationnel sur les ports du commutateur et ne peut pas être commuté ou acheminé vers le réseau opérationnel.
- **Interface Management VLAN** : L'interface de gestion est l'interface logique utilisée pour la connectivité intrabande avec le commutateur sur l'une des interfaces réseau du commutateur. Pour accéder au commutateur sur un réseau, vous devez d'abord configurer une adresse IP et un masque de sous-réseau pour le commutateur.
- **Interface de gestion unique en option** : Par défaut, vous pouvez utiliser n'importe quelle interface réseau du commutateur comme interface de gestion. Cependant, vous pouvez restreindre la gestion IPv4 à une interface réseau spécifique.

Configurez le port de service IPv4

Vous pouvez configurer les informations réseau sur le port de service IPv4, également appelé port hors bande (OOB). Le port de service est un port Ethernet dédié pour la gestion hors bande du commutateur. Le trafic sur ce port est séparé du trafic réseau opérationnel sur les ports du commutateur et ne peut pas être commuté ou acheminé vers le réseau opérationnel.

Par défaut, aucune adresse IP n'est définie pour le port OOB, mais son client DHCP est activé pour que le port puisse recevoir une adresse IP d'un serveur DHCP de votre réseau. Si le port OOB ne reçoit pas d'adresse IP d'un serveur DHCP de votre réseau, l'adresse IP du port est définie sur 192.168.0.239 avec 255.255.255.0 comme masque de sous-réseau. Il en va de même si vous connectez le port OOB directement à un ordinateur et redémarrez le commutateur.

Pour configurer le port de service IPv4 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > gestion > interfaces de gestion > Configuration du port de service IPv4**.

La page Configuration du port de service IPv4 s'affiche.

6. Sélectionnez un bouton radio Service Port Configuration Protocol :

- **BOOTP** Au cours du cycle de démarrage suivant, le client BootP sur le périphérique diffuse une requête BootP pour acquérir des informations à partir d'un serveur BootP sur le réseau.

Les informations des champs adresse IP, masque de sous-réseau et passerelle par défaut sont acquises dynamiquement.

- **DHCP** Au cours du cycle de démarrage suivant, le client DHCP sur le périphérique diffuse une requête DHCP pour acquérir des informations à partir d'un serveur DHCP sur le réseau.

Les informations des champs adresse IP, masque de sous-réseau et passerelle par défaut sont acquises dynamiquement.

- **Aucun** : Le périphérique ne tente pas d'acquérir des informations réseau de manière dynamique. Vous devez configurer les paramètres d'adresse manuellement :
 - **IP Address** (Adresse IP). Spécifiez l'adresse IP de l'interface.
 - **Subnet Mask** (Masque de sous-réseau). Masque de sous-réseau IP de l'interface.
 - **Passerelle par défaut** Passerelle par défaut pour l'interface IP.

7. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 16 : Informations de configuration du port de service IPv4

Champ	Description
Adresse MAC gravée	Adresse MAC gravée utilisée pour la connectivité hors bande.
État de l'interface	Indique si l'état de la liaison est actif ou inactif.
Identifiant client DHCP	Si la sélection est DHCP, l'ID client DHCP.

Configurez un VLAN de gestion IPv4

Pour gérer le commutateur sur l'interface utilisateur principale, vous devez définir l'adresse IP de gestion. Une interface VLAN de gestion est créée par défaut et informatique obtient une adresse IP si un serveur DHCP est présent. Si l'interface VLAN de gestion ne peut pas obtenir d'adresse IP, l'adresse IPv4 de secours automatiquement attribuée est 169.254.100.100 et le masque de sous-réseau est 255.255.0,0.

Un VLAN de gestion est utilisé comme interface source par défaut pour le syslog, le journal des messages, un client SNMP, etc. L'interface réseau est désactivée par défaut.

Le VLAN de gestion est l'interface logique utilisée pour la connectivité intrabande avec le commutateur via l'un des ports du panneau avant du commutateur. Les paramètres de configuration associés à l'interface réseau du commutateur n'affectent pas la configuration des ports du panneau avant par lesquels le trafic est commuté ou acheminé.

Pour accéder au commutateur sur un réseau, vous devez d'abord configurer une adresse IP et un masque de sous-réseau pour le commutateur. Vous pouvez configurer les informations IP à l'aide de l'une des méthodes suivantes :

- DHCP
- Interface de terminal via le port EIA-232

Une fois la connectivité intrabande établie, vous pouvez modifier les informations IP à l'aide de l'une des méthodes suivantes :

- Interface de terminal via le port EIA-232
- Interface de terminal via Telnet
- Gestion basée sur SNMP
- Administration Web

Pour configurer un VLAN de gestion IPv4 ou réinitialiser le VLAN de gestion IPv4 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > gestion > interfaces de gestion > Configuration VLAN de gestion IPv4**.

La page Configuration de l'VLAN de gestion IPv4 s'affiche.

6. Dans le champ **ID VLAN de gestion**, spécifiez l'ID VLAN de gestion du commutateur.

Le VLAN de gestion est utilisé pour gérer le switch. Vous pouvez configurer n'importe quelle valeur comprise entre 1 et 4093.

7. Sélectionnez le bouton radio **Activer** ou **désactiver** le mode de routage pour activer ou désactiver le routage global sur le commutateur.

La valeur par défaut est Activer.

8. Sélectionnez le bouton radio méthode de configuration **DHCP** ou **Manuel** pour spécifier l'action de démarrage du commutateur :

- DHCP Le commutateur demande des informations d'adresse IP à un serveur DHCP.
- Manuel Le commutateur charge les informations d'adresse IP que vous spécifiez :
 - **IP Address** (Adresse IP). Spécifiez l'adresse IP de l'interface.

La valeur par défaut est 169 254 100 100.

- **Subnet Mask** (Masque de sous-réseau). Masque de sous-réseau IP de l'interface. Il est également appelé masque de sous-réseau/réseau et définit la partie de l'adresse IP de l'interface utilisée pour identifier le réseau connecté.

La valeur par défaut est 255.255.0,0.

- Passerelle : Spécifiez la passerelle de l'interface.

La valeur par défaut est 0,0,0,0.

9. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

! Remarque: Si vous devez réinitialiser l'VLAN de gestion IPv4, dans la section Réinitialiser l'interface de gestion IPv4 de la page, cochez la case **définir l'interface de gestion sur la valeur par défaut** et cliquez sur le bouton **appliquer**. Cela supprime la configuration de l'interface de gestion IPv4 basée sur les ports et rétablit l'interface de gestion IPv4 sur la valeur par défaut VLAN 1.

La section Etat actuel de l'interface de gestion IPv4 affiche les champs en lecture seule suivants.

Table 17 : Informations sur l'état de l'interface de gestion IPv4

Champ	Description
Interface d'administration	Affiche le VLAN de gestion IPv4 actuel
Etat du lien	Indique si l'état de la liaison est actif ou inactif
État de l'interface de routage	Indique si l'état de la liaison est actif ou inactif pour l'interface de gestion
Adresse MAC	Adresse MAC attribuée à l'interface de gestion
Méthode de configuration de l'adresse IP	Indique si la méthode de configuration de l'adresse IP est DHCP ou manuelle
Adresse IP	Adresse IP de l'interface de gestion
Masque de sous-réseau	Masque de sous-réseau IP de l'interface.
Passerelle	Passerelle par défaut spécifiée pour l'interface de gestion

Configurer une interface de gestion IPv4

Vous pouvez restreindre la gestion IPv4 à une interface spécifique. Par défaut, vous pouvez utiliser n'importe quelle interface comme interface de gestion IPv4.

Pour configurer une interface de gestion IPv4 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > gestion > interfaces de gestion > Configuration de l'interface de gestion IPv4**.

La page Configuration de l'interface de gestion IPv4 s'affiche.

6. Dans le menu **interface**, sélectionnez l'interface qui doit devenir l'interface de gestion IPv4.
7. Cochez la case **définir l'option interface de gestion** pour pouvoir configurer les paramètres d'adresse IP de l'interface
8. Sélectionnez une case d'option méthode de configuration :
 - DHCP Le commutateur obtient les paramètres d'adresse IP de l'interface de gestion à partir d'un serveur DHCP du réseau.
 - Manuel Configurez manuellement les paramètres d'adresse IP de l'interface de gestion :

- **IP Address** (Adresse IP). Spécifiez l'adresse IP de l'interface de gestion.
- **Subnet Mask** (Masque de sous-réseau). Spécifiez le masque de sous-réseau de l'interface de gestion.
- **Passerelle** : Spécifiez l'adresse IP de la passerelle par défaut pour l'interface de gestion.

9. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

! Remarque: Si vous devez réinitialiser l'interface de gestion IPv4, dans la section Réinitialiser l'interface de gestion IPv4 de la page, cochez la case définir l'interface de gestion par défaut et cliquez sur le bouton **appliquer**. Cela supprime la configuration de l'interface de gestion IPv4 et rétablit le paramètre par défaut de l'interface de gestion IPv4.

La section interface de gestion IPv4 actuelle affiche les champs en lecture seule suivants.

Table 18 : Informations sur l'état de l'interface de gestion IPv4

Champ	Description
Interface d'administration	Affiche l'interface de gestion IPv4 actuelle
Etat du lien	Indique si l'état de la liaison est actif ou inactif
État de l'interface de routage	Indique si l'état de la liaison est actif ou inactif pour l'interface de gestion
Adresse MAC	Adresse MAC attribuée à l'interface de gestion
Méthode de configuration de l'adresse IP	Indique si la méthode de configuration de l'adresse IP est DHCP ou manuelle
Adresse IP	Adresse IP de l'interface de gestion
Masque de sous-réseau	Masque de sous-réseau IP de l'interface.
Passerelle	Passerelle par défaut spécifiée pour l'interface de gestion

Interfaces de gestion IPv6 et VLAN

L'interface utilisateur principale fournit des options distinctes pour l'interface IPv6 et la gestion IP basée sur les ports.

Si vous configurez la gestion IP basée sur les ports, la gestion IP basée sur VLAN est désactivée. De même, si vous configurez la gestion IP basée sur VLAN, la gestion IP basée sur les ports est désactivée.

Par défaut, l'interface source des applications est VLAN 1. Si vous modifiez l'VLAN et le port de gestion IPv6 sur une valeur autre que celle par défaut, l'interface source sur l'VLAN et le port par défaut VLAN 1 sont également automatiquement modifiés.

Vous pouvez accéder au commutateur sur l'interface utilisateur principale par l'une des méthodes suivantes :

- **Port de service IPv6** : Le port de service est un port Ethernet dédié pour la gestion hors bande du commutateur. Le trafic sur ce port est séparé du trafic réseau opérationnel sur les ports du commutateur et ne peut pas être commuté ou acheminé vers le réseau opérationnel.
- **Interface Management VLAN** : L'interface de gestion est l'interface logique utilisée pour la connectivité intrabande avec le commutateur sur l'une des interfaces réseau du commutateur. Pour accéder au commutateur sur un réseau, vous devez d'abord configurer une adresse IP et un masque de sous-réseau pour le commutateur. Pour configurer un VLAN de gestion IPv6, vous pouvez utiliser le même VLAN que celui utilisé pour la gestion IPv4 ou un VLAN différent. Le commutateur ne fournit pas de VLAN de gestion IPv6 par défaut. Si vous voulez en utiliser un, vous devez créer informatique manuellement.
- **Interface de gestion unique en option** : Par défaut, vous pouvez utiliser n'importe quelle interface réseau du commutateur comme interface de gestion. Cependant, vous pouvez restreindre la gestion IPv6 à une interface réseau spécifique.

Configurez un port de service IPv6

Vous pouvez configurer les informations réseau IPv6 sur le port de service. Le port de service est un port Ethernet dédié pour la gestion hors bande du trafic de commutateur sur ce port est séparé du trafic réseau opérationnel sur les ports de commutateur et ne peut pas être commuté ou acheminé vers le réseau opérationnel.

Pour configurer le port de service IPv6 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > gestion > interfaces de gestion > Configuration du port de service IPv6**.

La page Configuration du port de service IPv6 s'affiche.

6. Sélectionnez le bouton radio **Activer** ou **désactiver** le mode IPv6.

Ceci spécifie le mode administratif IPv6 sur le port de service.

7. Sélectionnez le bouton radio Service Port Configuration Protocol **None** ou **DHCP**.

Indique si le périphérique acquiert des informations réseau à partir d'un serveur DHCPv6. La sélection **de aucun** désactive le client DHCPv6 sur le port de service.

Si vous sélectionnez le bouton radio **DHCP**, le champ DUID du client DHCPv6 affiche l'identificateur de client utilisé par le client DHCPv6 lors de l'envoi de messages au serveur DHCPv6.

8. Sélectionnez le bouton radio **Activer** ou **désactiver** le mode de configuration automatique de l'adresse sans état IPv6 :

- Activer. Le port de service peut acquérir une adresse IPv6 via le protocole NDP (Neighbor Discovery Protocol) IPv6 et via l'utilisation de messages d'annonce de routeur.
- Désactiver : Le port de service n'utilise pas la fonction d'autoconfiguration d'adresse IPv6 native pour acquérir une adresse IPv6.

Ceci définit le mode d'autoconfiguration d'adresse IPv6 sans état sur le port de service.

9. Pour configurer la passerelle IPv6, procédez comme suit :

- a. Cochez la case **modifier la passerelle IPv6**.

La passerelle IPv6 est la passerelle par défaut pour l'interface de port de service IPv6.

- b. Dans le champ passerelle IPv6, spécifiez la passerelle par défaut pour l'interface réseau IPv6.

10. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

11. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Gérer les adresses IPv6 pour le port de service IPv6

Vous pouvez ajouter une adresse IPv6 statique spécifique au port de service IPv6. Vous pouvez également supprimer une adresse IPv6 dont vous n'avez plus besoin pour le port de service IPv6.

Pour ajouter ou supprimer une adresse IPv6 pour le port de service IPv6 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur principale à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **système > gestion > interfaces de gestion > Configuration du port de service IPv6**.
La page Configuration du port de service IPv6 s'affiche.
Le tableau Ajouter/Supprimer une adresse IPv6 répertorie les adresses IPv6 statiques que vous avez ajoutées manuellement à l'interface du port de service.
6. Pour ajouter une adresse IPv6, dans la section Ajouter/Supprimer une adresse IPv6, procédez comme suit :
 - a. Dans le champ **adresse IPv6**, spécifiez l'adresse IPv6 que vous souhaitez ajouter.
 - b. Dans le menu **INDICATEUR EUI**, sélectionnez **vrai** pour activer l'indicateur EUI (Extended Universal identifier) pour l'adresse IPv6 ou **faux** pour omettre l'indicateur.
 - c. Cliquez sur le bouton **Add** (Ajouter).

L'adresse IPv6 est ajoutée au port de service IPv6.
7. Pour supprimer une adresse IPv6, dans la section Ajouter/Supprimer une adresse IPv6, procédez comme suit :
 - a. Cochez la case correspondant à l'adresse IPv6 que vous souhaitez supprimer.
 - b. Cliquez sur le bouton **Supprimer**.

L'adresse IPv6 est supprimée du port de service IPv6.
8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez un VLAN de gestion IPv6

Pour gérer le commutateur sur l'interface utilisateur principale, vous devez définir l'adresse IP de gestion. Une interface VLAN de gestion est créée par défaut et informatique obtient une adresse IP si un serveur DHCP est présent. Si l'interface VLAN de gestion ne peut pas obtenir d'adresse IP, l'adresse IPv4 de secours automatiquement attribuée est 169.254.100.100 et le masque de sous-réseau est 255.255.0,0.

Un VLAN de gestion est utilisé comme interface source par défaut pour le syslog, le journal des messages, un client SNMP, etc. L'interface réseau est désactivée par défaut.

Le VLAN de gestion est l'interface logique utilisée pour la connectivité intrabande avec le commutateur via l'un des ports du panneau avant du commutateur. Les paramètres de configuration associés à l'interface réseau du commutateur n'affectent pas la

configuration des ports du panneau avant par lesquels le trafic est commuté ou acheminé.

Pour accéder au commutateur sur un réseau, vous devez d'abord configurer une adresse IP et un masque de sous-réseau pour le commutateur. Vous pouvez configurer les informations IP à l'aide de l'une des méthodes suivantes :

- DHCP
- Interface de terminal via le port EIA-232

Une fois la connectivité intrabande établie, vous pouvez modifier les informations IP à l'aide de l'une des méthodes suivantes :

- Interface de terminal via le port EIA-232
- Interface de terminal via Telnet
- Gestion basée sur SNMP
- Administration Web

Pour configurer un VLAN de gestion IPv6, vous pouvez utiliser le même VLAN que celui utilisé pour la gestion IPv4 ou un VLAN différent. Le commutateur ne fournit pas de VLAN de gestion IPv6 par défaut. Si vous voulez en utiliser un, vous devez créer informatique manuellement.

Pour configurer un VLAN de gestion IPv6 ou réinitialiser le VLAN de gestion IPv6 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **système > gestion > interfaces de gestion > Configuration VLAN de gestion IPv6** .
La page Configuration du VLAN de gestion IPv6 s'affiche.
6. Dans le champ **ID VLAN de gestion**, spécifiez l'ID VLAN de gestion du commutateur.
Le VLAN de gestion est utilisé pour gérer le switch. Vous pouvez configurer n'importe quelle valeur comprise entre 1 et 4093.
7. Sélectionnez le bouton radio Activer ou **désactiver** le mode IPv6 pour spécifier le mode d'administration pour le VLAN de gestion IPv6.
8. Sélectionnez le bouton radio **Activer** ou **désactiver** le mode de configuration automatique de l'adresse pour spécifier le mode de configuration automatique de l'adresse.

Si vous activez ce mode, les paramètres réseau IPv6 (préfixe IPv6 et longueur du préfixe) sont automatiquement configurés pour l'interface VLAN de gestion configurée. Par défaut, pour VLAN 1, le mode est activé pour que les paramètres soient automatiquement configurés.

❗ Remarque: L'option Address Autoconfigure mode est disponible uniquement si le routage monodiffusion est globalement désactivé.

9. Sélectionnez le bouton radio **Activer** ou **désactiver** le mode DHCP de l'adresse pour spécifier si les paramètres IPv6 sont obtenus à partir d'un serveur DHCP.
10. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
11. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

❗ Remarque: Si vous devez réinitialiser l'interface de gestion IPv6, dans la section Réinitialiser l'interface de gestion IPv6 de la page, cochez la case **définir l'interface de gestion par défaut** et cliquez sur le bouton **appliquer**. Cela supprime la configuration de l'interface de gestion IPv6.

La section Etat actuel de l'interface de gestion IPv6 affiche les champs en lecture seule suivants.

Table 19 : Informations sur l'état actuel de l'interface de gestion IPv6

Champ	Description
Interface d'administration	L'interface de gestion IPv6. (Par défaut, aucune interface de gestion IPv6 n'est configurée).
Etat du lien	Indique si l'état de la liaison est actif ou inactif.
État de l'interface de routage IPv6/mode opérationnel	Indique si l'état de la liaison est actif ou inactif pour l'interface de gestion IPv6.
Adresse MAC	Adresse MAC attribuée à l'interface de gestion IPv6.
Mode d'activation IPv6	Indique si IPv6 est activé ou désactivé sur l'interface de gestion IPv6.
Mode de routage IPv6	Indique si le routage IPv6 est activé ou désactivé sur l'interface de gestion IPv6.
Mode client DHCPv6	Indique si le mode client DHCPv6 est activé ou désactivé sur l'interface de gestion IPv6.
Passerelle IPv6 par défaut	Adresse IPv6 de la passerelle par défaut du commutateur.
Interface de saut suivant IPv6	Adresse IPv6 de l'interface du tronçon suivant du commutateur.
Préfixe IPv6/longueur du préfixe	Préfixe IPv6 et longueur de préfixe utilisés pour l'interface de gestion IPv6.
EU164	Drapeau EUI-64 de l'adresse IPv6 sur l'interface de gestion IPv6.
Etat actuel	État actuel de l'adresse IPv6 sur l'interface de gestion IPv6.

Gérer les adresses IPv6 pour le VLAN de gestion IPv6

Vous pouvez ajouter une adresse IPv6 statique spécifique au VLAN de gestion IPv6. Vous pouvez également supprimer une adresse IPv6 dont vous n'avez plus besoin pour le VLAN de gestion IPv6.

Pour ajouter ou supprimer une adresse IPv6 pour le VLAN de gestion IPv6 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > gestion > interfaces de gestion > Configuration VLAN de gestion IPv6** .

La page Configuration du VLAN de gestion IPv6 s'affiche.

Si le mode de configuration automatique de l'adresse est activé, le préfixe IPv6 et la longueur du préfixe sont affichés dans la section Configuration de l'interface IPv6 VLAN.

6. Pour ajouter une adresse IPv6, dans la section Configuration de l'interface VLAN IPv6, procédez comme suit :

- a. Dans le champ **longueur du préfixe IPv6**, spécifiez l'adresse IPv6 et la longueur du préfixe que vous souhaitez ajouter.
- b. dans le menu EUI64, sélectionnez vrai pour activer l'indicateur EUI (Extended Universal identifier) pour l'adresse IPv6 ou faux pour omettre l'indicateur EUI.
- c. Cliquez sur le bouton **Add** (Ajouter).

L'adresse IPv6 est ajoutée à l'VLAN de gestion IPv6.

7. Pour supprimer une adresse IPv6, dans la section Configuration de l'interface VLAN IPv6, procédez comme suit :

- a. Cochez la case correspondant à l'adresse IP et au préfixe à supprimer.
- b. Cliquez sur le bouton **Supprimer**.

L'adresse IPv6 est supprimée de l'VLAN de gestion IPv6.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Gérer les adresses de route IPv6 par défaut pour le VLAN de gestion IPv6

Vous pouvez ajouter une adresse de route IPv6 par défaut spécifique au VLAN de gestion IPv6. Vous pouvez également supprimer une adresse de route IPv6 par défaut dont vous n'avez plus besoin pour le VLAN de gestion IPv6.

Pour ajouter ou supprimer une adresse de route IPv6 par défaut pour le VLAN de gestion IPv6 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > gestion > interfaces de gestion > Configuration VLAN de gestion IPv6**.

La page Configuration du VLAN de gestion IPv6 s'affiche.

6. Pour ajouter une adresse de route IPv6 par défaut, dans la section Configuration de la route IPv6 par défaut, procédez comme suit :

- a. Cochez la case **modifier la route IPv6 par défaut**.
- b. Dans le champ **adresse de route IPv6 par défaut**, spécifiez l'adresse IPv6 et la longueur du préfixe que vous souhaitez ajouter.
- c. Cliquez sur le bouton **Add** (Ajouter).

L'adresse de route IPv6 par défaut est ajoutée à l'VLAN de gestion IPv6.

7. Pour supprimer une adresse de route IPv6 par défaut, dans la section Configuration de la route IPv6 par défaut, procédez comme suit :
 - a. Cochez la case correspondant à l'adresse de route IPv6 par défaut que vous souhaitez supprimer.
 - b. Cliquez sur le bouton **Supprimer**.

L'adresse de route IPv6 par défaut est supprimée de l'VLAN de gestion IPv6.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurer une interface de gestion IPv6

Vous pouvez restreindre la gestion IPv6 à une interface spécifique. Par défaut, vous pouvez utiliser n'importe quelle interface comme interface de gestion IPv6.

Pour configurer une interface de gestion IPv6 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > gestion > interfaces de gestion > Configuration de l'interface de gestion IPv6**.

La page Configuration de l'interface de gestion IPv6 s'affiche.

6. Dans le menu **interface**, sélectionnez l'interface qui doit devenir l'interface de gestion IPv6.
7. Cochez la case **définir l'option interface de gestion** pour pouvoir configurer les paramètres de l'interface.
8. Sélectionnez le bouton radio **Activer** ou **désactiver** le mode de routage pour activer ou désactiver le routage sur l'interface de gestion IPv6.
9. Sélectionnez le bouton radio **Activer** ou **désactiver** le mode IPv6 pour activer ou désactiver IPv6 sur l'interface de gestion IPv6.
10. Sélectionnez le bouton radio **Activer** ou **désactiver** le mode de configuration automatique des adresses sans état pour activer ou désactiver le mode de configuration automatique des adresses sans état sur l'interface de gestion IPv6.
Vous pouvez activer ce mode uniquement si le routage monodiffusion est globalement désactivé.
11. Sélectionnez le bouton radio **Activer** ou **désactiver** le mode client DHCPv6 pour activer ou désactiver le mode client DHCPv6 sur l'interface de gestion IPv6.
12. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

13. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

! Remarque: Si vous devez réinitialiser l'interface de gestion IPv6, dans la section Réinitialiser l'interface de gestion IPv6 de la page, cochez la case **définir l'interface de gestion par défaut** et cliquez sur le bouton **appliquer**. Cela supprime la configuration de l'interface de gestion IPv6.

La section Etat actuel de l'interface de gestion IPv6 affiche les champs en lecture seule suivants.

Table 20 : Informations sur l'état actuel de l'interface de gestion IPv6

Champ	Description
Interface d'administration	L'interface de gestion IPv6 (par défaut, aucune interface de gestion IPv6 n'est configurée)
Etat du lien	Indique si l'état de la liaison est actif ou inactif
État de l'interface de routage IPv6/mode opérationnel	Indique si l'état de la liaison est actif ou inactif pour l'interface de gestion IPv6
Adresse MAC	Adresse MAC attribuée à l'interface de gestion IPv6
Mode d'activation IPv6	Indique si IPv6 est activé ou désactivé sur l'interface de gestion IPv6
Mode de routage IPv6	Indique si le routage IPv6 est activé ou désactivé sur l'interface de gestion IPv6
Mode client DHCPv6	Indique si le mode client DHCPv6 est activé ou désactivé sur l'interface de gestion IPv6
Passerelle IPv6 par défaut	Adresse IPv6 de la passerelle par défaut du commutateur
Interface de saut suivant IPv6	Adresse IPv6 de l'interface du tronçon suivant du commutateur
Préfixe IPv6/longueur du préfixe	Préfixe IPv6 et longueur de préfixe utilisés pour l'interface de gestion IPv6
EU164	Drapeau EUI-64 de l'adresse IPv6 sur l'interface de gestion IPv6
Etat actuel	État actuel de l'adresse IPv6 sur l'interface de gestion IPv6

Gérer les adresses IPv6 pour l'interface de gestion IPv6

Vous pouvez ajouter une adresse IPv6 statique spécifique à l'interface de gestion IPv6. Vous pouvez également supprimer une adresse IPv6 dont vous n'avez plus besoin pour l'interface de gestion IPv6.

Pour ajouter ou supprimer une adresse IPv6 pour l'interface de gestion IPv6 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > gestion > interfaces de gestion > Configuration de l'interface de gestion IPv6**.

La page Configuration de l'interface de gestion IPv6 s'affiche.

6. Pour ajouter une adresse IPv6, dans la section Configuration de l'interface de gestion IPv6, procédez comme suit :

- a. Cochez la case **définir l'interface de gestion**.

informatique est probable que vous l'ayez déjà fait lorsque vous avez démarré la configuration de l'interface de gestion IPv6.

- b. Dans le champ **préfixe IPv6**, spécifiez l'adresse IPv6 à ajouter.
- c. Dans le champ **longueur du préfixe**, spécifiez la longueur du préfixe de l'adresse IPv6 que vous souhaitez ajouter.
- d. Dans le menu **EUI64**, sélectionnez **Activer** pour activer l'indicateur EUI (Extended Universal identifier) pour l'adresse IPv6 ou **désactiver** pour omettre l'indicateur.
- e. Cliquez sur le bouton **Add** (Ajouter).

L'adresse IPv6 est ajoutée à l'interface de gestion IPv6.

7. Pour supprimer une adresse IPv6, dans la section Configuration de l'interface de gestion IPv6, procédez comme suit :
 - a. Cochez la case correspondant à l'IPv6 que vous souhaitez supprimer.
 - b. Cliquez sur le bouton **Supprimer**.

L'adresse IPv6 est supprimée de l'interface de gestion IPv6.
8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Gérer les adresses de route IPv6 par défaut pour l'interface de gestion IPv6

Vous pouvez ajouter une adresse de route IPv6 par défaut spécifique à l'interface de gestion IPv6. Vous pouvez également supprimer une adresse de route IPv6 par défaut dont vous n'avez plus besoin pour l'interface de gestion IPv6.

Pour ajouter ou supprimer une adresse de route IPv6 par défaut pour l'interface de gestion IPv6 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > gestion > interfaces de gestion > Configuration de l'interface de gestion IPv6**.

La page Configuration de l'interface de gestion IPv6 s'affiche.

6. Pour ajouter une adresse de route IPv6 par défaut, dans la section Configuration de la route IPv6 par défaut, procédez comme suit :
 - a. Cochez la case **modifier la route IPv6 par défaut**.
 - b. Dans le champ **adresse de route IPv6 par défaut**, spécifiez l'adresse IPv6 et la longueur du préfixe que vous souhaitez ajouter.
 - c. Cliquez sur le bouton **Add** (Ajouter).

L'adresse de route IPv6 par défaut est ajoutée à l'interface de gestion IPv6.

7. Pour supprimer une adresse de route IPv6 par défaut, dans la section Configuration de la route IPv6 par défaut, procédez comme suit :
 - a. Cochez la case correspondant à l'adresse de route IPv6 par défaut que vous souhaitez supprimer.
 - b. Cliquez sur le bouton **Supprimer**.

L'adresse de route IPv6 par défaut est supprimée de l'interface de gestion IPv6.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Paramètres heure et NTP

Le commutateur prend en charge le protocole NTP (Network Time Protocol), qui est un protocole de synchronisation des horloges des systèmes informatiques en réseau, principalement lorsque le transfert de données est géré via Internet.

Configurez les paramètres NTP globaux

Pour configurer les paramètres NTP globaux :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > gestion > heure > Configuration de l'heure** .

La page Configuration de l'heure s'affiche.

Les champs date et heure affichent la date et l'heure actuelles détectées par le commutateur.

6. Sélectionnez le bouton radio **Activer** ou **désactiver** le mode d'authentification NTP pour activer ou désactiver l'authentification des paquets NTP sur le commutateur.

Lorsque cette option est activée, un paquet NTP provenant d'un serveur NTP est authentifié. L'authentification est basée sur SHA256. Si le paquet ne peut pas être authentifié, l'ordinateur est abandonné et le commutateur ne peut pas synchroniser son heure avec le serveur NTP qui a envoyé le paquet.

Par défaut, ce mode est activé.

7. Sélectionnez le bouton radio **Activer** ou **désactiver** le mode client de diffusion NTP pour activer ou désactiver la diffusion des requêtes NTP par le commutateur vers un serveur NTP.

La diffusion d'une requête NTP peut toujours être utile s'il n'y a pas de serveur NTP public configuré sur le commutateur parce que l'ordinateur permet au commutateur de synchroniser son heure avec un serveur NTP qui est accessible dans le réseau,

par opposition à un serveur de temps externe, tel qu'un serveur de temps public. Par défaut, ce mode est désactivé.

8. Dans le champ **délai de diffusion**, spécifiez le délai d'aller-retour estimé en microsecondes entre le client NTP et le serveur de diffusion NTP.

La plage est de 1 à 999999. Le numéro par défaut est 3000.

Le délai est la période perdue entre la requête sortante et la réponse entrante en raison du trafic réseau et du routage. Le commutateur ajoute le délai que vous spécifiez à l'heure que l'ordinateur reçoit du serveur NTP afin que le commutateur puisse calculer l'heure réelle.

9. Dans le menu **interface source**, sélectionnez l'interface sortante.

Le client NTP utilise l'adresse IP source de cette interface pour diffuser les requêtes NTP. Par défaut, les options suivantes s'affichent dans le menu :

- Aucun : Adresse IP principale de l'interface d'origine (sortante)
- VLAN 1 Adresse IP principale de VLAN 1. Il s'agit de la sélection par défaut.
- Port de service Adresse IP du port de gestion

Selon la configuration de votre commutateur, les options suivantes peuvent s'afficher :

- **Un autre identifiant VLAN** : Adresse IP principale d'un VLAN autre que VLAN 1
- **Interface de routage** : Adresse IP principale d'une interface de routage
- VLAN de routage Adresse IP principale d'une interface de routage VLAN
- **Interface de bouclage de routage** : Adresse IP principale d'une interface de bouclage de routage
- **Différent**: Pour certaines fonctionnalités, *différents* peuvent s'afficher. Cela signifie que l'interface source est configurée séparément.

10. Dans le champ **nom du fuseau horaire**, spécifiez un fuseau horaire.

Dans les champs **heures de décalage** et **minutes de décalage**, vous pouvez spécifier le nombre d'heures et de minutes pendant lesquelles le fuseau horaire est différent du temps universel coordonné (UTC). Le fuseau horaire peut affecter l'affichage de l'heure actuelle du système.

! Remarque: Lorsque vous utilisez un serveur de temps NTP public, les données de temps qui sont reçues du serveur sont basées sur UTC, qui est le même que Greenwich Mean Time (GMT). Il ne s'agit peut-être pas du fuseau horaire dans lequel se trouve le commutateur, mais du fuseau horaire dans lequel vous souhaitez que le commutateur fonctionne.

11. Dans le champ heures de décalage, spécifiez le nombre d'heures pendant lesquelles le fuseau horaire est différent de l'UTC.

La plage est de -12 à 14. Le numéro par défaut est 0.

12. Dans le champ minutes de décalage, spécifiez le nombre de minutes pendant lesquelles le fuseau horaire est différent de UTC.

La plage est de 0 à 59. Le numéro par défaut est 0.

13. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

14. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Affiche l'état NTP global et les informations sur les paquets

Vous pouvez afficher l'état NTP global et les informations sur les paquets.

Pour afficher l'état NTP global et les informations sur les paquets :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur principale à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > gestion > heure > Configuration de l'heure**.

La page Configuration de l'heure s'affiche.

6. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

La section État global NTP affiche les champs en lecture seule suivants.

Table 21 : Informations d'état global NTP

Champ	Description
Version	Version NTP prise en charge par le client
Modes pris en charge	Modes NTP pris en charge par le client. Plusieurs modes peuvent être pris en charge par un client.
Adresse IP du serveur	Adresse IP du serveur de synchronisation pour le dernier paquet valide reçu. Si aucun message n'a été reçu d'un serveur, une chaîne vide est affichée.
Type d'adresse	Type d'adresse de l'adresse du serveur de synchronisation pour le dernier paquet valide reçu
Strate de serveur	Strate revendiquée du serveur de temps pour le dernier paquet valide reçu
ID horloge de référence	Identificateur d'horloge de référence du serveur de temps pour le dernier paquet valide reçu
Mode serveur	Mode du serveur de temps pour le dernier paquet valide reçu
Nombre maximal d'entrées du serveur de monodiffusion	Nombre maximal d'entrées de serveur de monodiffusion pouvant être configurées pour ce client
Entrées actuelles du serveur de monodiffusion	Nombre d'entrées de serveur monodiffusion valides actuellement configurées pour ce client

La section informations NTP affiche les champs en lecture seule suivants.

Table 22 : Informations NTP

Champ	Description
Nom du logiciel NTP	Nom de l'application logicielle NTP
Version du logiciel NTP	Version de l'application logicielle NTP
Type de système NTP	Informations sur la plate-forme du système d'exploitation du système NTP

La section paquets NTP affiche les champs en lecture seule suivants.

Table 23 : Informations sur les paquets NTP

Champ	Description
NTP en paquets	Nombre de messages NTP reçus par le commutateur
Paquets de sortie NTP	Nombre de messages NTP envoyés par le commutateur
Paquets de l'ancienne version NTP	Nombre de messages NTP pour une version NTP non prise en charge que le commutateur a reçus
Paquets d'erreur de protocole NTP	Nombre de messages NTP avec une erreur de protocole NTP que le commutateur a reçus

Configurer les serveurs NTP

NTP assure une synchronisation temporelle précise pour l'horloge du périphérique réseau, jusqu'à la milliseconde. La synchronisation temporelle est effectuée par un serveur NTP réseau. Le commutateur fonctionne comme un client NTP uniquement et ne fournit pas de services de temps aux autres périphériques.

Les sources de temps sont établies par strates. Les strates définissent la précision de l'horloge de référence. Plus la strate est élevée (zéro étant le plus élevé), plus l'horloge est précise. Le commutateur reçoit le temps des périphériques de la strate 1 ou de la strate 0 car il est lui-même un périphérique de la strate 2.

Voici des exemples de strates :

- Strate 0. • Strate 0. Une horloge en temps réel est utilisée comme source de temps, par exemple, un système GPS.
- Strate 1. • Strate 1. Un serveur qui est directement lié à une source de temps strate 0 est utilisé. Les serveurs de temps Stratum 1 fournissent des normes de temps réseau primaires.
- Strate 2. La source de temps est distante du serveur de strate 1 sur un chemin de réseau. Par exemple, un serveur de strate 2 reçoit le temps sur une liaison réseau, via NTP, d'un serveur de strate 1.

Les informations reçues des serveurs NTP sont évaluées en fonction du niveau de temps et du type de serveur.

Les définitions de temps NTP sont évaluées et déterminées par les niveaux de temps suivants :

- T1 : Heure à laquelle la demande initiale a été envoyée par le client.
- T2 : Heure à laquelle le serveur a reçu la demande d'origine.
- T3 : Heure à laquelle le serveur a envoyé une réponse.
- T4 : Heure à laquelle le client a reçu la réponse du serveur.

T1 à T4 sont utilisés pour déterminer l'heure du serveur.

Le périphérique peut interroger les types de serveur de monodiffusion pour l'heure du serveur. Le commutateur interroge les informations de monodiffusion afin de détecter un serveur dont l'adresse IP est connue. Les serveurs NTP qui ont été configurés sur le périphérique sont les seuls qui sont interrogés pour obtenir des informations de synchronisation. Il s'agit de la méthode préférée pour synchroniser l'heure du périphérique car c'est la méthode la plus sécurisée.

Le dispositif récupère des informations de synchronisation, soit en demandant activement des informations, soit à chaque intervalle d'interrogation.

Ajoutez un serveur NTP

Le commutateur est préconfiguré avec des serveurs NTP publics, mais vous pouvez également ajouter des serveurs NTP.

Pour ajouter un serveur NTP :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez système > gestion > heure > Configuration du serveur NTP.

La page Configuration du serveur NTP s'affiche.

6. Dans le menu type de serveur, sélectionnez le type d'adresse NTP à saisir dans le champ d'adresse.
L'adresse peut être une adresse IPv4, une adresse IPv6 ou un nom d'hôte (DNS). La valeur par défaut est DNS.
7. Dans le champ adresse, spécifiez l'adresse IP ou le nom d'hôte du serveur NTP.
Il s'agit d'une chaîne de texte de 64 caractères maximum, contenant l'adresse IP unicast codée ou le nom d'hôte d'un serveur NTP. Les requêtes NTP unicast sont envoyées à cette adresse. L'adresse est un nom d'hôte DNS, puis ce nom d'hôte est résolu en une adresse IP chaque fois qu'une requête NTP lui est envoyée.
8. Dans le champ **version**, spécifiez la version NTP prise en charge par le commutateur.
La plage est de 1 à 4. Le numéro par défaut est 4.
9. Dans le champ **ID de clé**, spécifiez le numéro de clé d'authentification que le commutateur utilise pour communiquer avec le serveur NTP.
La plage est de 0 à 4294967295.
10. Dans le champ **intervalle d'interrogation minimum**, spécifiez l'intervalle d'interrogation le plus court en puissances de deux secondes.
La gamme est comprise entre 2^4 et 2^{17} . La valeur par défaut est 2^6 .
11. Dans le champ **intervalle d'interrogation maximal**, spécifiez l'intervalle d'interrogation le plus long en puissances de deux secondes.
La gamme est comprise entre 2^4 et 2^{17} . La valeur par défaut est 2^{10} .
12. Dans le menu **Préférer**, sélectionnez **Oui** pour attribuer le serveur NTP comme serveur NTP préféré.
Un serveur préféré réduit le nombre de fois que le commutateur doit changer entre différents serveurs NTP. La valeur par défaut est non, ce qui signifie qu'un serveur NTP n'est pas un serveur préféré.
13. Dans le menu **rafale**, sélectionnez **Oui** pour permettre au commutateur d'envoyer une série de paquets au lieu d'un seul paquet dans chaque intervalle de synchronisation.
Si vous sélectionnez non, un seul paquet est envoyé, ce qui peut ralentir la synchronisation. La valeur par défaut est Oui.
14. Dans le menu **iBurst**, sélectionnez **Oui** pour permettre au commutateur d'envoyer une série de paquets au lieu d'un seul paquet dans l'intervalle de synchronisation initial.
Si vous sélectionnez non, un seul paquet est envoyé, ce qui peut ralentir la synchronisation initiale. La valeur par défaut est Oui.
15. Cliquez sur le bouton **Add** (Ajouter).
L'entrée du serveur NTP est ajoutée.

16. Pour ajouter des serveurs NTP supplémentaires, répétez les étapes précédentes.
17. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau associations de serveurs NTP affiche les informations suivantes.

Table 24 : Informations sur les associations de serveur NTP

Champ	Description
Nom de l'association	Adresse IP ou nom d'hôte de l'association NTP
ID de référence	ID de référence de l'association NTP
Type de serveur	Type d'adresse (IPv4 ou IPv6) pour l'association
Adresse	Adresse IPv4 ou IPv6 de l'association
Décalage	Temps de décalage pour l'association.
Strate	La version strate de l'association
Gigue	Gigue en millisecondes pour l'association
Délai	Délai réseau en millisecondes pour l'association
Dispersion	Dispersion racine (facteur d'erreur) pour l'association.
NTP en paquets	Nombre de messages NTP que le commutateur a reçus pour l'association
Paquets de sortie NTP	Nombre de messages NTP envoyés par le commutateur pour l'association
Paquets d'erreur de protocole NTP	Nombre de messages NTP avec une erreur de protocole NTP que le commutateur a reçus pour l'association

Modifiez les paramètres d'un serveur NTP existant

Vous pouvez modifier le paramètre d'un serveur NTP préconfiguré ou personnalisé existant.

Pour modifier les paramètres d'un serveur NTP existant :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez système > gestion > heure > Configuration du serveur NTP.
La page Configuration du serveur NTP s'affiche.
6. Dans la section Configuration du serveur NTP, cochez la case en regard du serveur NTP.
7. Modifiez les paramètres en fonction de vos besoins.
8. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimez un serveur NTP

Vous pouvez supprimer une règle de trafic dont vous n'avez plus besoin.

Pour supprimer un serveur NTP :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez système > gestion > heure > Configuration du serveur NTP.
La page Configuration du serveur NTP s'affiche.
6. Dans la section Configuration du serveur NTP, cochez la case en regard du serveur NTP.
7. Cliquez sur le bouton **Supprimer**.
Le serveur est supprimé.
8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurer les paramètres de l'heure d'été

Vous pouvez configurer les paramètres de l'heure d'été, également appelée heure d'été. Utilisé dans certains pays du monde, l'heure d'été est la pratique d'avancer temporairement les horloges pendant les mois d'été. Typiquement, les horloges sont réglées vers l'avant une ou plusieurs heures près du début du printemps et sont réglées vers l'arrière en automne.

Pour configurer les paramètres de l'heure d'été :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > gestion > heure > Configuration de l'heure d'été** .

La page Configuration de l'heure d'été s'affiche.

6. Sélectionnez l'un des boutons radio heure d'été (DST) suivants :

- Désactiver : Désactiver l'heure d'été.
- Récurrent L'heure d'été a lieu à la même heure chaque année. Vous devez configurer manuellement les heures et dates de début et de fin du décalage horaire.

Configurez les paramètres décrits dans [Étape 7](#).

- UE récurrente L'horloge système utilise les paramètres d'heure d'été récurrente standard utilisés dans les pays de l'Union européenne. Avec cette option, les autres champs applicables de la page sont automatiquement renseignés et vous ne pouvez pas les modifier.

Configurez les paramètres décrits dans [Étape 7](#).

- États-Unis récurrents L'horloge système utilise les paramètres d'heure d'été récurrents standard utilisés aux États-Unis. Avec cette option, les autres champs applicables de la page sont automatiquement renseignés et vous ne pouvez pas les modifier.

Configurez les paramètres décrits dans [Étape 7](#).

- **Non récurrent** : Les paramètres d'heure d'été ne sont en vigueur qu'entre la date de début et la date de fin de l'année spécifiée. Lorsque cette option est sélectionnée, les réglages de l'heure d'été ne se répètent pas sur une base annuelle.

Configurez les paramètres décrits dans Étape 8.

7. Si vous sélectionnez le bouton radio **récurrent**, **récurrent eu** ou **récurrent USA** , configurez les champs indiqués dans le tableau suivant.

Champ	Description
Commence à	Ces champs sont utilisés pour configurer les valeurs de début de la date et de l'heure. • Semaine Configurez la semaine de début. • Jour Configurez le jour de début. • Mois Configurez le mois de début. • Heures Configurez les heures de début. • Minutes Configurez les minutes de début.
Se termine à	Ends t ces champs sont utilisés pour configurer les valeurs de fin de date et d'heure. • Semaine Configurez la semaine de fin. • Jour Configurez le jour de fin. • Mois Configurez le mois de fin. • Heures Configurez les heures de fin. • Minutes Configurez les minutes de fin.
Décalage	Configurer le décalage récurrent en minutes. La plage valide est comprise entre 1 et 1440 minutes.
Zone	Configurez le fuseau horaire.

8. Si vous sélectionnez **non récurrent**, configurez les champs indiqués dans le tableau suivant.

Champ	Description
Commence à	Ces champs sont utilisés pour configurer les valeurs de début de la date et de l'heure. • Mois Configurez le mois de début. • Date Configurez la date de début. • Année Configurez l'année de début. • Heures Configurez les heures de début. • Minutes Configurez les minutes de début.
Se termine à	Ends t ces champs sont utilisés pour configurer les valeurs de fin de date et d'heure. • Mois Configurez la date de début de fin. • Date Configurez la date de fin. • Année Configurez l'année de fin. • Heures Configurez les heures de fin. • Minutes Configurez les minutes de fin.
Décalage	Configurez le décalage non récurrent en minutes. La plage valide est comprise entre 1 et 1440 minutes.
Zone	Configurez le fuseau horaire.

9. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Afficher l'état de l'heure d'été

Vous pouvez afficher des informations sur les paramètres de l'heure d'été et si le décalage horaire pour l'heure d'été est actuellement en vigueur.

Pour afficher l'état de l'heure d'été :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > gestion > heure > Configuration de l'heure d'été**.

La page Configuration de l'heure d'été s'affiche.

6. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

Le tableau suivant affiche les informations d'état de l'heure d'été (heure d'été) en lecture seule.

Table 25 : Informations sur l'état de l'heure d'été

Champ	Description
Heure d'été (DST)	La valeur de l'heure d'été, qui est l'une des valeurs suivantes : • Désactiver • Récurrent • UE récurrente • États-Unis récurrents • Non récurrent
Commence à	Affiche le début de l'heure d'été. Ce champ ne s'affiche pas lorsque l'heure d'été est désactivée.
Se termine à	S'affiche à la fin de l'heure d'été. Ce champ ne s'affiche pas lorsque l'heure d'été est désactivée.
Décalage (en minutes)	Valeur de décalage en minutes. Ce champ ne s'affiche pas lorsque l'heure d'été est désactivée.
Zone	Acronyme de zone. Ce champ ne s'affiche pas lorsque l'heure d'été est désactivée.
Heure d'été (DST) en vigueur	Indique si l'heure d'été est en vigueur.

Horloge transparente a protocole temporel de PRECISION

Precision Time Protocol (PTP, IEEE 1588) est un protocole qui permet une synchronisation précise des horloges avec une précision inférieure à la microseconde sur un réseau à base de paquets. Le protocole PTP permet aux périphériques réseau de précision et de résolution différentes de se synchroniser sur une horloge de grand maître via un échange de paquets à travers le réseau. Le commutateur prend en charge une horloge transparente (TC) PTP de bout en bout, qui est activée par défaut, à la fois globalement et au niveau du port.

Les modèles M4350-16V4C et M4350-40X4C prennent également en charge les fonctions d'horloge limite PTP et d'horloge grand maître (voir [Horloge limite de protocole de temps de précision et horloge grand maître](#) à la page 139).

❗ Remarque: Le commutateur lui-même n'est pas affecté par PTP.

❗ Remarque: Pour les commutateurs compatibles SMPTE de la série M4350, vous pouvez configurer PTP-BC et PTP-TC sur différents ports du même commutateur, à condition que chaque type de PTP se trouve sur un VLAN distinct. Pour obtenir la liste des commutateurs compatibles SMPTE de la série M4350, reportez-vous aux [switchs manageables AV et informatique NETGEAR](#).

Gérer les paramètres PTP TC globaux

Par défaut, l'horloge transparente (TC) PTP de bout en bout est activée globalement sur le commutateur. Vous pouvez désactiver PTP TC globalement, auquel cas le commutateur ne prend pas en charge l'intercommunication PTP.

Pour configurer les paramètres PTP (TC) globalement :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > gestion > PTP TC > Configuration globale**.

La page Configuration globale s'affiche.

6. Sélectionnez le bouton radio **Activer** ou **désactiver** le mode Admin.

La valeur par défaut est Activer.

7. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Gérer les paramètres de l'interface PTP TC

Sur un commutateur autonome, par défaut, l'horloge transparente (TC) PTP de bout en bout est activée globalement sur toutes les interfaces. Dans une pile de commutateurs, par défaut, PTP TC est désactivé pour toutes les interfaces. Vous pouvez sélectionner des interfaces individuelles sur lesquelles vous pouvez activer ou désactiver PTP TC. Si vous désactivez PTP TC sur une interface, celle-ci ne prend pas en charge l'intercommunication PTP.

Pour configurer les paramètres PTP TC pour une ou plusieurs interfaces :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > gestion > PTP TC > Configuration de l'interface** .

La page Configuration de l'interface s'affiche.

6. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :

- **1 ou ID d'unité pour un commutateur empilé :**
 - 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
 - **ID d'unité pour un commutateur empilé :** Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
- **LAG** Seuls les LAG sont affichés.
- **Tous:** Les interfaces physiques et les LAG sont affichés, ou pour une pile de commutateurs, les interfaces physiques de tous les commutateurs de la pile et les LAG sont affichés.

7. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :

- Pour afficher ou effacer les statistiques d'une seule interface, cochez la case associée à l'interface ou saisissez le numéro de l'interface dans le champ **aller à l'interface** et cliquez sur le bouton **aller**.
 - Pour configurer plusieurs interfaces avec les mêmes paramètres, cochez la case associée à chaque interface.
 - Pour configurer toutes les interfaces avec les mêmes paramètres, cochez la case dans la ligne d'en-tête.
8. Dans le menu du mode EEE, sélectionnez Activer ou désactiver.
La valeur par défaut est Activer.
9. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
Le champ mode de fonctionnement indique si le protocole PTP est activé ou désactivé pour une interface.
10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Horloge limite de protocole de temps de précision et horloge grand maître

❗ Remarque: Les fonctions d'horloge limite PTP et d'horloge grand maître sont prises en charge sur les modèles M4350-16V4C et M4350-40X4C uniquement.

Precision Time Protocol (PTP, IEEE 1588) est un protocole qui permet une synchronisation précise des horloges avec une précision inférieure à la microseconde sur un réseau à base de paquets. Le protocole PTP permet aux périphériques réseau de précision et de résolution différentes de se synchroniser sur une horloge de grand maître via un échange de paquets à travers le réseau.

Le commutateur prend en charge une horloge limite (BC) et une horloge grand maître (GM). Par défaut, le mode BC PTP est désactivé sur les modèles M4350-16V4C et M4350-40X4C. Ces deux modèles sont capables de fonctionner comme une horloge GM PTP.

Les horloges peuvent être définies comme suit :

- **Horloge frontière (BC) :** Commutateur doté d'un port qui fonctionne comme émetteur de temps (maître) dans un réseau PTP et d'un ou plusieurs autres ports

qui fonctionnent comme récepteurs de temps. Selon la valeur de priorité de l'horloge locale et d'autres paramètres, la fonction d'horloge de commutation dans un réseau PTP peut changer automatiquement de l'horloge limite à l'horloge grand maître.

- **Grandmaster (GM) horloge** : Commutateur doté d'un port qui fonctionne comme source de temps et émetteur de temps (maître) dans un réseau PTP. L'horloge grand maître fournit une référence temporelle précise pour un ou plusieurs dispositifs directement reliés au commutateur et synchronisant leurs horloges avec l'horloge grand maître. Selon la valeur de priorité de l'horloge locale et d'autres paramètres, la fonction d'horloge de commutation dans un réseau PTP peut changer automatiquement de l'horloge grand maître à l'horloge limite.

Le meilleur algorithme d'horloge maître (BMCA) détermine le meilleur émetteur temporel (maître) pour un domaine PTP et détermine la hiérarchie émetteur-récepteur temporel avec le meilleur émetteur temporel comme racine.

Notez ce qui suit au sujet de la fonction d'horloge PTP BC/GM :

- Si un profil réseau utilisant AVB est activé (voir [802.1AS synchronisation et synchronisation](#) à la page 490), l'horloge BC PTP (ou horloge transparente) est automatiquement désactivée et vous ne pouvez pas activer manuellement la fonction. AVB et PTP ne peuvent pas coexister.
- PTP n'est pas pris en charge sur une pile.

❗ Remarque: Pour les commutateurs compatibles SMPTE de la série M4350, vous pouvez configurer PTP-BC et PTP-TC sur différents ports du même commutateur, à condition que chaque type de PTP se trouve sur un VLAN distinct. Pour obtenir la liste des commutateurs compatibles SMPTE de la série M4350, reportez-vous aux [switchs manageables AV et informatique NETGEAR](#).

Gérez les paramètres de l'horloge limite PTP globale et de l'horloge grand maître

Par défaut, le mode horloge limite PTP et horloge grand maître est désactivé sur le commutateur. Vous pouvez activer le mode et configurer les paramètres globaux du commutateur.

Pour gérer l'horloge limite PTP et le mode horloge grand maître et configurer les paramètres globaux :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > gestion > PTP > Configuration globale PTP**.

La page Configuration globale PTP s'affiche.

6. Sélectionnez le bouton radio **Activer** ou **désactiver** le mode Admin.

La valeur par défaut est désactiver.

7. Dans le champ **priorité de l'horloge locale1**, entrez une valeur de priorité comprise entre 0 et 255. La priorité 1 détermine quel commutateur capable de fonctionner comme horloge grand maître est choisi comme horloge grand maître active dans le réseau.

8. Dans le champ **priorité de l'horloge locale2**, entrez une valeur comprise entre 0 et 255. La priorité 2 détermine également quel commutateur capable de fonctionner comme horloge grand maître est choisi comme horloge grand maître active dans le réseau.

9. En fonction des besoins de votre réseau, sélectionnez l'un des boutons radio suivants pour un profil d'horloge PTP :

- Par défaut Les paramètres PTPv2 par défaut sont utilisés. Il s'agit de l'option par défaut.
- AES67 : Profil d'horloge permettant de connecter des périphériques audio sur un profil PTP commun.

- SMPTE-2059-2 : Profil d'horloge pour le trafic vidéo.
- AES-R16-2016 : Profil d'horloge qui interagit entre les profils d'horloge SMPTE et AES67.

10. Dans le champ **intervalle d'annonce**, entrez la période entre les messages d'annonce successifs au format logarithme en base 2.

Les messages d'annonce aident à élire la meilleure horloge de grand maître dans le réseau. Voici les plages prises en charge et les paramètres par défaut pour les profils d'horloge PTP :

- Par défaut 0 à 4. Le paramètre par défaut est 1.
- AES67 : 0 à 4. Le paramètre par défaut est 1.
- SMPTE-2059-2 : -3 à 1. Le paramètre par défaut est 0.
- AES-R16-2016 : 0 ou 1. Le paramètre par défaut est 0.

11. Il s'agit du nombre de messages d'annonce qui ne sont pas acquittés avant que le commutateur ne détermine que l'horloge grand maître n'est pas en train de transmettre.

Vous pouvez définir un nombre compris entre 2 et 10. Le paramètre par défaut pour tous les profils d'horloge PTP est 3. Pour le profil AES-R16-2016, la seule valeur possible est 3.

12. Dans le champ **intervalle de synchronisation**, entrez la période entre les messages de synchronisation successifs, au format logarithme en base 2.

Voici les plages prises en charge et les paramètres par défaut pour les profils d'horloge PTP :

- Par défaut -1 à 1. Le paramètre par défaut est 0.
- AES67 : -4 à 1. Le paramètre par défaut est -3.
- SMPTE-2059-2 : -7 à -1. Le paramètre par défaut est -3.
- AES-R16-2016 : -4 à 1. Le paramètre par défaut est -3.

13. Dans le champ **intervalle de demande de retard**, entrez la période entre les messages de demande de retard successifs de l'horloge limite à l'horloge grand-maître, au format logarithme en base 2.

Les messages Delay-Request aident à calculer le délai de chemin. Voici les plages prises en charge et les paramètres par défaut pour les profils d'horloge PTP :

- Par défaut 0 à 5. Le paramètre par défaut est 0.
- AES67 : -3 à 5. Le paramètre par défaut est 0.
- SMPTE-2059-2 : -7 à 4. Le paramètre par défaut est -3.
- AES-R16-2016 : -4 à 5. Le paramètre par défaut est -3.

14. Sélectionnez le bouton radio **IPv4**, **IPv6** ou **L2 transport** pour définir le protocole de transport à utiliser sur le chemin de communication.
 15. Dans le champ **taille MTU**, entrez une valeur comprise entre 0 et 127.

Un domaine PTP se compose d'une horloge ordinaire ou périphérique communiquant entre elles, et d'une horloge grand maître unique. Bien que plusieurs commutateurs puissent fonctionner comme grand maître dans le réseau, un seul commutateur peut utiliser l'horloge grand maître active.
 16. Dans le menu **niveau de journalisation PTP**, sélectionnez le niveau de journalisation pour les transitions d'état PTP et l'état.

Les options sont **urgence**, **alerte**, **critique**, **erreur**, **avertissement**, **remarque** (paramètre par défaut), **Info** et **Déboguer**. Les messages de journal avec le niveau de gravité sélectionné et tous les messages de journal de gravité supérieure sont consignés. Par exemple, si vous sélectionnez avertissement, les messages consignés incluent avertissement, erreur, critique, alerte et urgence.
 17. Sélectionnez le bouton radio PTP Path-trace **Activer** ou **désactiver**.

Une trace de chemin est la route qu'un message d'annonce PTP emprunte à travers le chemin réseau des horloges limites et est suivie à travers le TLV de trace de chemin dans le message d'annonce. La séquence de trace de chemin contient l'identité d'horloge de chaque horloge limite traversée par un message d'annonce. La valeur par défaut est désactiver.
 18. Dans le champ **adresse IPv4 source**, saisissez l'adresse IPv4 du port qui fonctionne comme horloge limite ou grand maître.

Par défaut, l'adresse source IPv4 du paquet PTP est dérivée de l'interface de routage sortant. Si l'interface sortante n'est pas activée pour le routage L3, vous devez spécifier l'adresse source PTP.
 19. Dans le champ **adresse IPv6 source**, saisissez l'adresse IPv6 du port qui fonctionne comme horloge limite ou grand-maître.

Par défaut, l'adresse source IPv6 du paquet PTP est dérivée de l'interface de routage sortant. Si l'interface sortante n'est pas activée pour le routage L3, vous devez spécifier l'adresse source PTP.
 20. Sélectionnez un bouton radio mode de fonctionnement de l'horloge :
 - **Une étape** : L'horloge horodatage le message Sync lorsqu'il quitte le port.
 - **En deux étapes**: L'horloge horodatage le message Sync lorsqu'il quitte le port, puis suit immédiatement avec un autre message qui capture l'horodatage de sortie du message Sync. Il s'agit de l'option par défaut.
 21. Dans le champ **étendue de la destination de multidiffusion IPv6**, saisissez l'étendue de la destination de multidiffusion IPv6 pour l'horloge périphérique ou grand-maître.

Par défaut, l'étendue de destination multicast IPv6 est 0xE.
 22. Sélectionnez le bouton radio **2,0** ou **2,1** pour définir la version PTP.
-

La version PTP par défaut est 2,1.

❗ **Remarque:** Les modèles M4350-16V4C et M4350-40x4C peuvent envoyer des paquets PTP à l'aide de la version PTP 2,0 en mode d'horloge limite.

23. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

24. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 26 : Informations de configuration globale PTP

Champ	Description
Processus PTP en cours d'exécution	Indique si le processus PTP est activé sur le commutateur.
Grandmaster capable	Indique si le commutateur est capable de devenir une horloge grand maître.
Modèle de communication	Ce champ est toujours Multicast.
Identité de l'horloge locale	ID de l'horloge, en utilisant un numéro EUI-64 attribué.

Gérer les paramètres de l'interface de l'horloge limite PTP

Sur un commutateur autonome, par défaut, la capacité d'horloge limite PTP est désactivée sur toutes les interfaces.

Pour configurer la capacité de l'horloge limite pour une ou plusieurs interfaces :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > gestion > PTP > Configuration de l'interface PTP**.

La page Configuration de l'interface PTP s'affiche.

6. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :

- Pour afficher ou effacer les statistiques d'une seule interface, cochez la case associée à l'interface ou saisissez le numéro de l'interface dans le champ **aller à l'interface** et cliquez sur le bouton **aller**.
- Pour configurer plusieurs interfaces avec les mêmes paramètres, cochez la case associée à chaque interface.
- Pour configurer toutes les interfaces avec les mêmes paramètres, cochez la case dans la ligne d'en-tête.

7. Dans le menu du mode EEE, sélectionnez Activer ou désactiver.

La valeur par défaut est désactiver.

8. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 27 : Informations sur la configuration de l'interface de l'horloge limite PTP et de l'horloge grand maître

Champ	Description
Mode de fonctionnement	Indique si l'horloge limite PTP et l'horloge grand maître sont activées ou désactivées pour une interface.
Etat du port	L'état de l'interface, qui est NA par défaut. L'état peut être l'un des suivants : Initialisation, écoute, défectueux, Désactivé, pré-maître, maître, passif, non étalonné ou récepteur de temps.
Compatible PTP	Indique si l'interface est capable de devenir une horloge limite ou une horloge grand maître.

Afficher ou effacer les statistiques de l'horloge limite PTP

Vous pouvez afficher ou effacer les statistiques de l'horloge limite PTP pour les interfaces.

Pour afficher ou effacer les statistiques d'horloge limite PTP pour les interfaces :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > gestion > PTP > statistiques PTP** .

La page statistiques PTP s'affiche.

6. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :

- Pour afficher ou effacer les statistiques d'une seule interface, cochez la case associée à l'interface ou saisissez le numéro de l'interface dans le champ **aller à l'interface** et cliquez sur le bouton **aller**.
- Pour effacer les statistiques de plusieurs interfaces, cochez la case associée à chaque interface.
- Pour effacer les statistiques de toutes les interfaces, cochez la case dans la ligne d'en-tête.

7. Pour effacer les statistiques, cliquez sur le bouton **Effacer**.

Les statistiques de l'interface ou des interfaces sélectionnées sont effacées.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 28 : Informations statistiques sur l'horloge limite PTP et l'horloge grand maître

Champ	Description
Interface	Interface pour laquelle les informations sont affichées.
Annonce	
Transféré	Nombre de messages d'annonce transmis.
Reçu	Nombre de messages d'annonce reçus.
Dépassement du délai imparti	Le nombre de messages d'annonce qui ont expiré.
Sync	
Transféré	Nombre de messages Sync transmis.
Reçu	Le nombre de messages Sync reçus.
Non-correspondance	Le nombre de messages de synchronisation qui ne correspondent pas.
Dépassement du délai imparti	Le nombre de messages de synchronisation qui ont expiré.
Suivi	
Transféré	Nombre de messages de suivi transmis.
Reçu	Nombre de messages de suivi reçus.
Non-correspondance	Nombre de messages de suivi qui ne correspondent pas.

Table 28 : Informations statistiques sur l'horloge limite PTP et l'horloge grand maître (A continué)

Champ	Description
Délai requis	
Transféré	Nombre de messages de délai requis transmis.
Reçu	Nombre de messages de demande de délai reçus.
Délai Rés	
Transféré	Nombre de messages Delay Res transmis.
Reçu	Nombre de messages Delay Res reçus.
Intensité	
Transféré	Nombre de messages de signalisation transmis.
Reçu	Nombre de messages de signalisation reçus.
Administration	
Transféré	Nombre de messages de gestion transmis.
Reçu	Nombre de messages de gestion reçus.

Afficher des informations détaillées sur l'horloge limite PTP

Vous pouvez afficher des informations détaillées sur l'état de l'horloge limite PTP sur le commutateur.

Pour afficher des informations détaillées sur l'état de l'horloge limite PTP :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > gestion > PTP > Détails PTP**.

La page Détails PTP s'affiche.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 29 : Informations détaillées sur l'horloge limite PTP et l'horloge grand maître

Champ	Description
PTP parent, horloge parent	
Identité de l'horloge	Valeur d'identité d'horloge de l'horloge parent.
Décalage	Variance logarithmique décalée de l'horloge parent.
Taux de changement de phase de l'horloge	La valeur du taux de changement de phase de l'horloge parent.
Parent PTP, horloge Grandmaster	
Identité de l'horloge	Valeur d'identité d'horloge de l'horloge grand maître.
Classe d'horloge	Valeur de classe d'horloge de l'horloge grand maître.
Précision de l'horloge	La valeur de précision de l'horloge du grand maître.
Décalage	Variance logarithmique décalée de l'horloge grand maître.
Priority1	La valeur de priorité 1 configurée de l'horloge grand maître.
Priority2	La valeur de priorité 2 configurée de l'horloge grand maître.
Horloge limite PTP	
Type de périphérique PTP	Type de périphérique PTP, qui peut être une horloge ordinaire, une horloge transparente ou une horloge limite.
Profil de périphérique PTP	Profil de périphérique, qui correspond au profil d'un périphérique spécifique dans un réseau spécifique.

Table 29 : Informations détaillées sur l'horloge limite PTP et l'horloge grand maître (A continué)

Champ	Description
Type de rôle d'horloge PTP	Le rôle de l'horloge limite peut être l'horloge maîtresse ou l'horloge du récepteur de temps.
Mode de fonctionnement de l'horloge	Le mode de fonctionnement de l'horloge limite PTP configurée, qui peut être une ou deux étapes.
Mode de fonctionnement de l'horloge parent	Le mode de fonctionnement de l'horloge parent, qui peut être N/A pour l'horloge maître ou à une ou deux étapes pour l'horloge du récepteur de temps. Si l'état n'est pas connu, le champ affiche non disponible.
Domaine d'horloge	Domaine configuré auquel appartient l'horloge limite.
Nombre de ports PTP	Nombre de ports PTP disponibles pour le fonctionnement PTP.
Classe d'horloge	Valeur de classe d'horloge de l'horloge limite.
Précision de l'horloge	La valeur de précision de l'horloge limite.
Décalage	Variance logarithmique décalée de l'horloge limite.
Étapes supprimées	Nombre de sauts que l'horloge grand-maître est supprimée de l'horloge limite PTP.
Délai moyen du chemin	Délai de bout en bout calculé, qui ne s'applique pas au PTP. Le champ affiche 0,0.
Propriétés de temps PTP	
Décalage UTC actuel	Valeur de décalage du temps universel coordonné (UTC).
Leap59	1 indique que la dernière minute de la journée contient 59 secondes. 0 indique que l'échelle de temps n'est pas PTP.
Leap61	1 indique que la dernière minute de la journée contient 61 secondes. 0 indique que l'échelle de temps n'est pas PTP.
Décalage UTC actuel valide	1 indique que la valeur de décalage UTC actuelle, la valeur Leap59 et la valeur Leap61 sont connues pour être correctes. 0 indique que ces valeurs sont inconnues ou inconnues pour être correctes.
Echelle de temps PTP	1 indique que l'échelle de temps PTP est traçable à une référence primaire. 0 indique que l'échelle de temps PTP n'est pas traçable.
Temps traçable	1 indique que l'échelle de temps est traçable à une référence primaire. 0 indique que l'échelle de temps n'est pas traçable.
Fréquence traçable	1 indique que la fréquence déterminant l'échelle de temps est traçable à une référence primaire. 0 indique que la fréquence déterminant l'échelle de temps n'est pas traçable.
Source de temps	Source de l'heure utilisée par l'instance PTP GM.

Table 29 : Informations détaillées sur l'horloge limite PTP et l'horloge grand maître (A continué)

Champ	Description
PTP Path-trace	
Identité de l'horloge	Une trace de chemin est la route qu'un message d'annonce PTP emprunte à travers le chemin réseau des horloges limites et est suivie à travers le TLV de trace de chemin dans le message d'annonce. La séquence de trace de chemin contient l'identité d'horloge de chaque horloge limite traversée par un message d'annonce.

Système de noms de domaine

Vous pouvez configurer des informations sur les serveurs DNS utilisés par le réseau et sur le fonctionnement du commutateur en tant que client DNS.

Configurez les paramètres DNS globaux et ajoutez un serveur DNS

Vous pouvez configurer les paramètres DNS globaux et les informations du serveur DNS.

Pour configurer les paramètres DNS globaux et ajouter un serveur DNS :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez système > gestion > DNS > Configuration DNS.

L'écran DNS Configuration (Configuration IP) s'affiche.

6. Sélectionnez le bouton radio **désactiver** ou **Activer** l'état DNS :

- Activer. Autorisez le commutateur à envoyer des requêtes DNS à un serveur DNS pour résoudre un nom de domaine DNS. La valeur par défaut est Activer.
- Désactiver : Empêcher le commutateur d'envoyer des requêtes DNS.

7. Dans le champ **DNS Default Name**, entrez le nom qui doit être inclus dans les requêtes DNS.

Lorsque le commutateur recherche un nom d'hôte non qualifié, ce champ fournit le nom de domaine. Par exemple, si le nom de domaine par défaut est netgear.com et que vous entrez test, test est remplacé par test.netgear.com pour résoudre le nom). La longueur maximale d'un nom d'utilisateur est de 255 caractères.

8. Dans le champ **numéro de nouvelle tentative**, spécifiez le nombre de tentatives que le commutateur doit effectuer pour envoyer des requêtes DNS au serveur DNS.

Entrez un nombre compris entre 0 et 100. Le numéro par défaut est 2.

9. Dans le champ **délai de réponse (secondes)**, spécifiez le temps en secondes pendant lequel le commutateur doit attendre une réponse à une requête DNS.

Entrez un nombre compris entre 0 et 3600. Le numéro par défaut est 3.

10. Dans le menu **source interface**, sélectionnez l'interface qui doit être l'interface source pour DNS, ce qui signifie que l'adresse IP principale de l'interface est utilisée comme adresse source. Par défaut, les options suivantes s'affichent dans le menu :

- Aucun : Adresse IP principale de l'interface d'origine (sortante)
- VLAN 1 Adresse IP principale de VLAN 1. Il s'agit de la sélection par défaut.
- Port de service Adresse IP du port de gestion

Selon la configuration de votre commutateur, les options suivantes peuvent s'afficher :

- **Un autre identifiant VLAN** : Adresse IP principale d'un VLAN autre que VLAN 1
- **Interface de routage** : Adresse IP principale d'une interface de routage
- **VLAN de routage** : Adresse IP principale d'une interface de routage VLAN
- **Interface de bouclage de routage** : Adresse IP principale d'une interface de bouclage de routage
- **Différent** : Pour certaines fonctionnalités, *différents* peuvent s'afficher. Cela signifie que l'interface source est configurée séparément.

11. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

12. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

13. Pour ajouter un serveur DNS auquel le commutateur envoie des requêtes DNS, procédez comme suit :

- a. Dans le champ **adresse du serveur DNS** du tableau Configuration du serveur DNS, entrez une adresse IP en notation IPv4 ou IPv6 standard.
- b. Cliquez sur le bouton **Add** (Ajouter).

L'entrée est ajoutée au tableau. Vous pouvez spécifier jusqu'à huit serveurs DNS. La priorité est définie dans l'ordre dans lequel vous ajoutez les serveurs.

14. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant affiche les informations du serveur DNS en lecture seule.

Table 30 : Informations sur la configuration du serveur DNS

Champ	Description
Numéro de série	Numéro de séquence du serveur DNS.
Préférences	Affiche la préférence du serveur DNS. La préférence est déterminée par l'ordre dans lequel vous ajoutez les serveurs.

Supprimer un serveur DNS

Vous pouvez supprimer une règle de trafic dont vous n'avez plus besoin.

Pour supprimer un serveur DNS :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez système > gestion > DNS > Configuration DNS.

L'écran DNS Configuration (Configuration IP) s'affiche.

6. Dans le tableau Configuration du serveur DNS, cochez la case correspondant au serveur DNS.

 **Attention:** Si vous ne sélectionnez pas de serveur DNS, tous les serveurs DNS sont supprimés lorsque vous cliquez sur le bouton **Supprimer**.

7. Cliquez sur le bouton **Supprimer**.

Le serveur DNS est supprimé.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurer et afficher les informations de nom d'hôte en adresse IP.

Vous pouvez mapper manuellement des noms d'hôte sur des adresses IP ou afficher des mappages d'hôte dynamiques.

Ajoutez une entrée statique à la table de mappage dynamique des hôtes

Pour ajouter une entrée statique à la table de mappage d'hôte dynamique local :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez système > gestion > DNS > Configuration hôte.

La page Configuration de l'hôte DNS s'affiche.

6. Dans le champ **nom d'hôte**, spécifiez le nom d'hôte statique.

La longueur maximale d'un nom d'utilisateur est de 255 caractères.

7. Dans le champ adresse IPv4/IPv6, entrez l'adresse IP à associer au nom d'hôte.
8. Cliquez sur le bouton **Add** (Ajouter).
L'entrée s'affiche dans le tableau Dynamic Host Mapping.
9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimez une entrée de la table de mappage dynamique des hôtes

Si vous n'êtes plus une entrée, vous pouvez supprimer informatique de la table de mappage dynamique des hôtes.

Pour supprimer une entrée de la table de mappage dynamique des hôtes :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.
4. Cliquez sur le bouton **Login** (Connexion).
La page System Information (Informations système) s'affiche.
5. Sélectionnez système > gestion > DNS > Configuration hôte.
La page Configuration de l'hôte DNS s'affiche.

6. Cochez la case en regard du morceau que vous souhaitez supprimer.
7. Cliquez sur le bouton **Supprimer**.
L'entrée est supprimée.
8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Maintenez la table de mappage dynamique des hôtes et affichez les entrées

Vous pouvez modifier le nom d'hôte ou l'adresse IP dans une entrée de la table de mappage dynamique des hôtes, afficher toutes les entrées ou effacer toutes les entrées.

Pour modifier le nom d'hôte ou l'adresse IP dans une entrée de la table de mappage dynamique des hôtes, affichez toutes les entrées ou effacez toutes les entrées :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.
4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez système > gestion > DNS > Configuration hôte.
La page Configuration de l'hôte DNS s'affiche.

6. Cochez la case en regard de l'entrée à mettre à jour.
7. Saisissez les nouvelles informations dans le champ approprié.
8. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
9. Pour effacer toutes les entrées de nom d'hôte dynamique de la liste, cliquez sur le bouton Effacer.
10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau Dynamic Host Mapping affiche les entrées de nom d'hôte en adresse IP apprises par le commutateur. Le tableau suivant décrit les champs d'hôte dynamique.

Table 31 : Informations de mappage dynamique des hôtes

Champ	Description
Hôte	Répertorie le nom d'hôte que vous attribuez à l'adresse IP spécifiée.
Total	Temps écoulé depuis que l'entrée dynamique a été ajoutée pour la première fois à la table.
Temps écoulé	Temps écoulé depuis la dernière mise à jour de l'entrée dynamique.
Type	Type de l'entrée dynamique.
Adresse	Répertorie l'adresse IP associée au nom d'hôte.

Changer de modèle de gestion de base de données

Un modèle de gestion de base de données de commutateur (SDM) détermine les ressources maximales que le commutateur peut utiliser pour diverses fonctions. En sélectionnant un modèle SDM en fonction de la façon dont vous utilisez le commutateur dans votre réseau, vous configurez le commutateur pour qu'il utilise un facteur d'échelle spécifique, qui détermine l'allocation des ressources. Autrement dit, en sélectionnant un modèle SDM, vous réaffectez les ressources du commutateur pour prendre en charge une combinaison spécifique de fonctionnalités en fonction des exigences de votre réseau.

L'interface utilisateur principale fournit plus d'informations sur les modèles (voir les étapes de cette tâche).

Le modèle SDM par défaut est IPv4-Basic. Vous pouvez modifier le modèle SDM du commutateur.

Pour modifier le modèle de module de détection et de diagnostic

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > gestion > préférence de modèle SDM**.

La page Préférences de modèle SDM s'affiche.

6. Dans le menu **ID modèle suivant SDM**, sélectionnez un modèle :

- **IPv4-Basic** (identique à **Default**) : Modèle pour un environnement IPv4 avec prise en charge d'IPv6 de base. Il s'agit du modèle par défaut.
- **IPv6-Basic** : Modèle pour un environnement IPv6 avec prise en charge d'IPv4 de base.
- **IPv4-BasicPlus** : Modèle pour un environnement IPv4 mettant l'accent sur le routage IPv4 unicast et multicast et la prise en charge d'IPv6. Ce modèle peut être utilisé pour n'importe quel modèle de commutateur M4350 à l'exception du modèle M4350-24G4XF.
- **IPv6-BasicPlus** : Modèle pour un environnement IPv6 mettant l'accent sur le routage IPv6 unicast et multicast et la prise en charge d'IPv4. Ce modèle peut

être utilisé pour n'importe quel modèle de commutateur M4350 à l'exception du modèle M4350-24G4XF.

7. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.
9. Pour activer le nouveau modèle, redémarrez le commutateur.
Le tableau suivant affiche des informations récapitulatives.

Table 32 : Informations récapitulatives sur le modèle SDM

Champ	Description
Modèle SDM	Identifie le modèle
Entrées ARP	Nombre maximal d'entrées dans le cache ARP (Address Resolution Protocol) pour les interfaces de routage
Routes IPv4 Unicast	Nombre maximal d'entrées de la table de transfert unicast IPv4
Entrées NDP IPv6	Nombre maximal d'entrées de cache NDP (Neighbor Discovery Protocol) IPv6
Routes IPv6 Unicast	Nombre maximal d'entrées de la table de transfert unicast IPv6
ECMP sauts suivants	Nombre maximal de sauts suivants pouvant être stockés dans les tables de transfert monodiffusion IPv4 et IPv6
Routes IPv4 Multicast	Nombre maximal d'entrées de la table de transfert multicast IPv4
Routes IPv6 Multicast	Nombre maximal d'entrées de la table de transfert multicast IPv6
Nombre maximum d'entrées VLAN	Le nombre maximum d'entrées VLAN, qui est de 4093 pour tout modèle SDM

Paramètres Ethernet verts

Vous pouvez configurer les fonctionnalités Ethernet verts pour réduire la consommation d'énergie globalement, ou sur une ou plusieurs interfaces, en passant en mode faible consommation lorsque les liaisons sont inactives.

Configurez les paramètres Ethernet verts globaux

Vous pouvez configurer les paramètres Ethernet verts globaux.

Pour configurer les paramètres Ethernet vert :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez système > gestion > Ethernet vert > Configuration Ethernet vert.

La page Green Ethernet Configuration s'affiche.

6. Sélectionnez le bouton radio désactiver ou Activer le mode de mise hors tension automatique.

Par défaut, ce mode est désactivé. Lorsqu'une liaison de port est interrompue, la couche physique sous-jacente est interrompue pendant une courte période, puis vérifie à nouveau les impulsions de liaison de port afin que la négociation automatique reste possible. De cette manière, le commutateur économise de l'énergie lorsqu'aucun partenaire de liaison n'est présent pour le port.

7. Sélectionnez le bouton radio désactiver ou Activer le mode EEE.

Par défaut, ce mode est désactivé. Energy Efficient Ethernet (EEE) combine le MAC avec une famille de couches physiques qui prennent en charge le fonctionnement en mode basse consommation. Il est défini par la norme IEEE 802.3az. Le mode d'économie d'énergie permet aux côtés envoi et réception de la liaison de désactiver certaines fonctionnalités d'économie d'énergie lorsque la charge est faible. Le

passage en mode faible consommation ne modifie pas l'état de la liaison. Les trames en transit ne sont pas perdues ou corrompues lors de la transition vers et depuis un port en mode faible consommation. Le temps de transition est transparent pour les protocoles et applications de couche supérieure.

8. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez les paramètres de l'interface Ethernet verte

Vous pouvez configurer des paramètres Ethernet verts pour des interfaces individuelles.

Pour configurer les paramètres de l'interface Ethernet verte :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.
4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.

5. Sélectionnez système > gestion > Ethernet vert > Configuration de l'interface Ethernet vert.

La page Green Ethernet Configuration s'affiche.

6. Si une pile est configurée, indiquez si vous souhaitez afficher les interfaces physiques d'un commutateur ou de tous les commutateurs de la pile :

- **ID d'unité pour un commutateur empilé** : Les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
Si aucune pile de commutateurs n'est configurée, la seule option est l'ID d'unité 1.
- **Tous** : Les interfaces physiques de tous les commutateurs de la pile sont affichées.
Si aucune pile de commutateurs n'est configurée, l'option tous n'a aucun effet.

7. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :

- Pour afficher ou effacer les statistiques d'une seule interface, cochez la case associée à l'interface ou saisissez le numéro de l'interface dans le champ **aller à l'interface** et cliquez sur le bouton **aller**.
- Pour configurer plusieurs interfaces avec les mêmes paramètres, cochez la case associée à chaque interface.
- Pour configurer toutes les interfaces avec les mêmes paramètres, cochez la case dans la ligne d'en-tête.

8. Dans le menu mode de mise hors tension automatique, sélectionnez Activer ou désactiver.

Par défaut, ce mode est désactivé pour le port. Lorsqu'une liaison de port est interrompue, la couche physique sous-jacente est interrompue pendant une courte période, puis vérifie à nouveau les impulsions de liaison de port afin que la négociation automatique reste possible. De cette manière, le commutateur économise de l'énergie lorsqu'aucun partenaire de liaison n'est présent pour le port. Si le mode mise hors tension automatique n'est pas pris en charge pour l'interface, N/A s'affiche.

9. Dans le menu du mode EEE, sélectionnez Activer ou désactiver.

Par défaut, ce mode est désactivé pour le port. Energy Efficient Ethernet (EEE) combine le MAC avec une famille de couches physiques qui prennent en charge le fonctionnement en mode basse consommation. Il est défini par la norme IEEE 802.3az. Le mode d'économie d'énergie permet aux côtés envoi et réception de la liaison de désactiver certaines fonctionnalités d'économie d'énergie lorsque la charge est faible. Le passage en mode faible consommation ne modifie pas l'état de la liaison. Les trames en transit ne sont pas perdues ou corrompues lors de la transition vers et depuis un port en mode faible consommation. Le temps de transition est transparent pour les protocoles et applications de couche supérieure.

10. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

11. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurer et afficher les paramètres Ethernet verts détaillés d'une interface

Vous pouvez sélectionner une interface unique et configurer et afficher les paramètres Ethernet verts détaillés.

Pour configurer et afficher les paramètres Ethernet verts détaillés pour une interface unique :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > gestion > Ethernet vert > Détails Ethernet vert**.

La page Green Ethernet Details s'affiche.

6. Dans le menu **interface**, sélectionnez l'interface.

7. Dans le menu **Energy Detect Admin mode**, sélectionnez pour activer ou désactiver ce mode.

Par défaut, ce mode est désactivé pour le port. Lorsqu'une liaison de port est interrompue, la couche physique sous-jacente est interrompue pendant une courte période, puis vérifie à nouveau les impulsions de liaison de port afin que la négociation automatique reste possible. De cette manière, le commutateur économise de l'énergie lorsqu'aucun partenaire de liaison n'est présent pour le port.

8. Dans le menu **EEE Admin mode**, sélectionnez pour activer ou désactiver ce mode. Lorsque le mode Energy Efficient Ethernet (EEE) est activé, le port passe en mode faible consommation lorsque la liaison est inactive. La valeur par défaut est Désactivé.
9. Dans le champ **EEE Transmit Idle Time**, entrez la période pendant laquelle l'interface doit rester inactive (sans recevoir de paquets pour la transmission) avant de passer à l'état Low-Power **Idle** (LPI).

La plage est de 600 à 4294967295 secondes. La valeur par défaut est de 600 secondes.

10. Dans le champ **EEE Transmit Wake Time**, entrez la période pendant laquelle l'interface reste à l'état LPI avant de revenir à l'état actif après que l'informatique ait reçu un paquet à transmettre.

La plage est de 8 à 65535 secondes. La valeur par défaut est de 17 secondes.

11. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

12. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 33 : Informations sur le périphérique local Ethernet vert

Champ	Description
Énergie cumulée économisée sur ce port grâce au(x) mode(s) vert(s) (Watts * heures)	Énergie cumulée économisée sur le port en raison des modes verts activés sur le port en watts * heures.
État opérationnel de détection d'énergie	État de fonctionnement (actif ou Inactif) du mode détection d'énergie.
Raison	Raison de l'état de fonctionnement affiché dans le champ précédent.
TW_sys_tx (usec)	La valeur de 'TW_sys' que le port peut prendre en charge.
Écho TW_sys_tx (usec)	Le « Transmit TW_sys » du partenaire de liaison que le port utilise pour calculer le « TW_sys » que l'informatique demande à son partenaire de liaison.
TW_sys_rx (usec)	La valeur de 'TW_sys' que le port a demandée à son partenaire de liaison.

Table 33 : Informations sur le périphérique local Ethernet vert (A continué)

Champ	Description
TW_sys_rx Echo (usec)	Le 'Receive TW_sys' du partenaire de liaison que le port utilise pour calculer le 'TW_sys' que informatique peut prendre en charge.
Fallback TW_sys (usec)	La valeur du paramètre « fallback TW_sys » que le port a demandé à son partenaire de liaison.
TX_DLL_enabled	État d'initialisation de la fonction Transmit EEE Transmit Data Link Layer (DLL) sur le port.
TX_DLL_Ready	L'état de la DLL de transmission, qui indique si l'initialisation du système tx est terminée et si le port est prêt à recevoir ou à mettre à jour des LLDPDU contenant des TLV EEE.
RX_DLL_enabled	État de la négociation de la capacité EEE sur le port.
RX_DLL_Ready	L'état de la DLL de réception, qui indique si l'initialisation du système rx est terminée et si le port est prêt à recevoir ou à mettre à jour des LLDPDU contenant des TLV EEE.
Temps écoulé depuis le dernier effacement des compteurs	Période écoulée depuis la réinitialisation des compteurs

Affiche des informations Ethernet vertes pour le partenaire de liaison d'une interface

Le commutateur peut détecter des informations Ethernet vertes pour le partenaire de liaison d'une interface, c'est-à-dire pour le périphérique distant.

Pour afficher les informations Ethernet vertes pour le partenaire de liaison d'une interface :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > gestion > Ethernet vert > Détails Ethernet vert**.

La page Green Ethernet Details s'affiche.

6. Faites défiler jusqu'à la section informations sur le périphérique distant.

7. Dans le menu **interface**, sélectionnez l'interface.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 34 : Informations sur le périphérique distant Ethernet vert

Champ	Description
ID distant	Identificateur attribué au partenaire de liaison du port.
Distant TW_sys_tx (usec)	La valeur de 'TW_sys' que le partenaire de liaison peut prendre en charge.
Écho TW_sys_tx distant (usec)	La valeur de 'Transmit TW_sys' que le partenaire de liaison renvoie au port.
Remote TW_sys_rx (usec)	La valeur de 'TW_sys' que le partenaire de liaison demande au port.
Écho TW_sys_rx distant (usec)	La valeur de 'receive TW_sys' que le partenaire de liaison renvoie au port.
Reprise d'appel distante TW_sys (usec)	La valeur de « fallback TW_sys » que le partenaire de liaison renvoie au port.

Affichez le résumé vert des statistiques Ethernet

Le récapitulatif vert des statistiques Ethernet affiche des informations sur le commutateur et les interfaces.

Pour afficher le résumé vert des statistiques Ethernet :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > gestion > Ethernet vert > Résumé Ethernet vert**.

La page Green Ethernet Summary s'affiche.

6. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

Le tableau suivant décrit les champs en lecture seule de la section Résumé des statistiques Ethernet vertes.

Table 35 : Informations récapitulatives sur les statistiques Ethernet vertes

Champ	Description
Consommation actuelle	Consommation électrique de tous les ports du commutateur en mWatts (mW).
Pourcentage d'économie d'énergie (%)	Pourcentage d'économie d'énergie sur tous les ports du commutateur lorsque le mode Ethernet vert est activé.
Économie d'énergie cumulée (W*H)	Énergie cumulée économisée sur le commutateur en (watts * heure) lorsque toutes les fonctions vertes sont activées.

Le tableau suivant décrit les champs en lecture seule de la section Récapitulatif des fonctions Ethernet vertes.

Table 36 : Informations récapitulatives sur la fonction Ethernet verte

Champ	Description
Unité	1, ou l'ID d'unité d'un commutateur empilé
Fonctions vertes prises en charge sur cet appareil	Fonctions vertes prises en charge par le commutateur : • Détection d'énergie • EEE (Energy Efficient Ethernet) • Historique LPI (historique d'inactivité à faible consommation d'énergie EEE) • LLDP-Cap-Exchg (échange de capacité EEE LLDP) • PWR-USG-est (estimations de consommation d'énergie).

Le tableau suivant décrit les champs en lecture seule de la section Récapitulatif de l'interface Ethernet verte.

Table 37 : Informations récapitulatives de l'interface Ethernet verte

Champ	Description
Interface	Interface pour laquelle les informations sont affichées.
Mode Admin détection d'énergie	Indique l'état du mode (Activer ou désactiver). Lorsqu'une liaison de port est interrompue, la couche physique sous-jacente est interrompue pendant une courte période, puis vérifie à nouveau les impulsions de liaison de port afin que la négociation automatique reste possible. De cette manière, le commutateur économise de l'énergie lorsqu'aucun partenaire de liaison n'est présent pour le port.
État opérationnel de détection d'énergie	État de fonctionnement (actif ou Inactif) du mode détection d'énergie.
EEE mode Admin	Indique l'état du mode (Activer ou désactiver). Si ce mode est activé, le port passe en mode faible consommation pendant une condition de liaison inactive.

Paramètres Bonjour

Un Mac prenant en charge Bonjour peut découvrir le commutateur dans le réseau afin que vous puissiez trouver l'adresse IP du commutateur et vous connecter à l'interface utilisateur principale du commutateur. Bonjour est activé par défaut. Vous pouvez désactiver NSDP pour des raisons de sécurité.

Activez ou désactivez Bonjour

Pour activer ou modifier Bonjour :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > gestion > Bonjour > Configuration Bonjour**.

La page Configuration Bonjour s'affiche.

6. Sélectionnez l'une des cases d'option suivantes :

- **Activer**. Bonjour est activé. Il s'agit de l'option par défaut.
- **Désactiver**. Bonjour est désactivé.

7. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Affiche les informations Bonjour

Pour afficher les informations Bonjour :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > gestion > Bonjour > Détails Bonjour** .

La page Bonjour Details s'affiche.

Le champ Bonjour Administration mode indique si Bonjour est activé ou désactivé.

6. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

Le tableau suivant décrit les champs en lecture seule de la page.

Table 38 : Bonjour Published services

Champ	Description
Nom du service	Noms de service Bonjour dans le commutateur.
Type	Noms de type de service Bonjour dans le commutateur.
Domaine	Domaine de service Bonjour dans le commutateur.

Table 38 : Bonjour Published services (A continué)

Champ	Description
Port	Numéro de port du service Bonjour.
Données TXT	Le texte du service Bonjour.

Activer ou désactiver la capacité du serveur TFTP

Par mesure de sécurité, la capacité du serveur TFTP (Trivial File Transfer Protocol) est désactivée par défaut sur le commutateur. Vous pouvez activer la capacité du serveur TFTP de sorte que le commutateur puisse atteindre un serveur TFTP si un serveur TFTP est configuré.

Pour activer ou désactiver la fonctionnalité du serveur TFTP :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > gestion > serveur TFTP**.

La page Configuration du serveur TFTP s'affiche.

6. Sélectionnez le bouton radio **Activer** ou **désactiver** le mode Admin.

La valeur par défaut est désactiver.

7. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Serveur DHCP IPv4

Vous pouvez configurer les paramètres d'un serveur DHCP IPv4, de pools DHCP et de liaisons DHCP. Vous pouvez également afficher les statistiques DHCP et, le cas échéant, les conflits DHCP.

Configurez un serveur DHCP

Pour configurer un serveur DHCP :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > services > serveur DHCP > Configuration du serveur DHCP**.

La page Configuration du serveur DHCP s'affiche.

6. Sélectionnez le bouton radio désactiver ou Activer le mode EEE.

Ce paramètre spécifie si le service DHCP est activé ou désactivé.

La valeur par défaut est désactiver.

7. Dans le champ **Ping Packet Count**, spécifiez le nombre de paquets qu'un serveur envoie à une adresse de pool pour vérifier la duplication dans le cadre d'une opération ping.

La valeur peut être 0 ou comprise entre 2 et 10. La définition de la valeur sur 0 désactive la fonction. Le numéro par défaut est 2.

8. Sélectionnez le bouton radio **désactiver** ou **Activer** le mode de journalisation des conflits.

Ce paramètre spécifie si la journalisation des conflits sur un serveur DHCP est activée ou désactivée. La valeur par défaut est Activer.

9. Sélectionnez le bouton radio BootP Automatic mode **Disable** ou **Enable**.

Ce paramètre spécifie si BootP pour les pools dynamiques est activé ou désactivé. La valeur par défaut est désactiver.

10. Pour exclure des adresses, procédez comme suit :

- a. Dans le champ **plage IP de**, saisissez l'adresse la plus basse de la plage ou une adresse unique à exclure.
- b. Dans le champ **plage IP à**, pour exclure une plage, entrez l'adresse la plus élevée de la plage. Pour exclure une seule adresse, entrez la même adresse IP que celle spécifiée dans le champ **plage IP de** ou laissez informatique sur 0,0.0,0.
- c. Cliquez sur le bouton **Add** (Ajouter).

Les adresses qui doivent être exclues sont ajoutées au commutateur.

11. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

12. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Ajoutez une classe DHCP à utiliser avec l'option DHCP 82

Si vous laissez le commutateur fonctionner comme un relais DHCP de couche 3, vous pouvez ajouter des classes DHCP et les configurer pour une utilisation avec les informations DHCP option 82. Il s'agit d'une fonction de sécurité qui permet au relais DHCP de détecter les informations de l'option DHCP 82 dans une requête DHCP et de transférer les requêtes uniquement à partir de périphériques approuvés. Pour plus d'informations sur l'utilisation du commutateur comme relais DHCP de couche 3, reportez-vous à la section Configurez les paramètres de relais DHCP globaux et affichez les statistiques de relais à la page 192.

Pour ajouter une classe DHCP à utiliser avec l'option DHCP 82 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **système > services > serveur DHCP > création de classe DHCP**.
La page création de classe de serveur DHCP s'affiche.
6. Dans le champ **nom de classe**, entrez un nom alphanumérique de 31 caractères maximum.
7. Cliquez sur le bouton **Add** (Ajouter).
Les paramètres sont enregistrés. La classe est ajoutée. Vous pouvez à présent configurer le switch.
8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez une classe DHCP

Pour chaque classe DHCP que vous ajoutez, vous pouvez configurer les sous-options ID distant et ID de circuit. Il s'agit de sous-options de l'option DHCP 82 qui limitent les périphériques pouvant recevoir une adresse IP du serveur DHCP.

Pour configurer une classe DHCP :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > services > serveur DHCP > Configuration de classe DHCP**

.

La page DHCP Class Configuration s'affiche.

6. Dans le menu **nom de classe**, sélectionnez la classe.
7. Dans le champ **ID distant**, spécifiez l'ID de l'hôte distant à partir duquel la demande DHCP peut être acceptée.

L'ID distant peut être un nom d'utilisateur, une ID d'appelant associée à un numéro de téléphone, une adresse ATM d'appelant, une ID de modem, une adresse IP, etc.

8. Dans le champ **ID du circuit**, spécifiez l'identifiant du circuit à partir duquel les requêtes DHCP peuvent être acceptées.

L'ID de circuit peut également être un numéro d'interface ou VLAN.

9. Cliquez sur le bouton **Add** (Ajouter).

Les paramètres sont enregistrés. La classe est ajoutée.

10. Pour ajouter un autre ensemble de sous-options pour la même classe, répétez les trois étapes précédentes.

11. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Gérer les pools DHCP

Vous pouvez configurer et gérer différents types de pools d'adresses IP que le serveur DHCP peut attribuer.

Créez un pool DHCP

Vous pouvez créer un pool DHCP et configurer plusieurs paramètres pour le pool.

Pour créer un pool DHCP :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > services > serveur DHCP > informations sur les conflits DHCP**.

La page DHCP Pool Configuration s'affiche.

6. Dans le menu **Pool Name (nom du pool)**, sélectionnez **Create(créer)**.

Le champ **Pool Name** s'affiche.

7. Dans le champ **nom du pool**, saisissez un nom pour le nouveau pool.

Le nom peut contenir jusqu'à 31 caractères.

8. Dans le menu **type de liaison**, sélectionnez le type de liaison pour le pool :

- Non alloué Aucune autre configuration n'est requise. Passez à l'étape suivante.
- Dynamique Configurez les paramètres suivants :

- Adresse réseau Adresse IP de sous-réseau du pool DHCP dynamique.
- Masque de réseau Masque réseau pour le pool DHCP dynamique.
- **Longueur du préfixe réseau** : Numéro de sous-réseau du pool DHCP dynamique. La plage est de 0 à 32.

❗ **Remarque:** Pour un pool DHCP dynamique, vous pouvez configurer le masque réseau ou la longueur du préfixe.

- Manuel Configurez les paramètres suivants :
 - **Nom du client** : Nom du client DHCP.
 - Adresse matérielle Adresse matérielle du client DHCP.
 - **Type d'adresse matérielle** : Protocole de l'adresse MAC du client DHCP. Le type peut être Ethernet ou IEEE802. La valeur par défaut est Ethernet.
 - ID de client ID client du client DHCP.
 - Numéro d'hôte Adresse IP pour la liaison manuelle du client DHCP.
 - **Masque hôte** : Masque de sous-réseau pour la liaison manuelle du client DHCP.
 - **Longueur du préfixe hôte** : Masque de sous-réseau pour la liaison manuelle du client DHCP. La plage est de 0 à 32.

❗ **Remarque:** Pour un client DHCP ajouté manuellement, vous pouvez configurer le masque réseau ou la longueur du préfixe.

9. Dans le menu **durée de location**, sélectionnez le mode de location de la reliure :
 - **Infini** : Pour une liaison dynamique, Infinite est une durée de location de 60 jours. Pour la liaison ajoutée manuellement, la période de bail est indéfinie. Aucune autre configuration n'est requise. Passez à l'étape suivante.
 - **Durée spécifiée** : Configurez les paramètres suivants :
 - **Jours**. Nombre de jours de la période de location. La plage est de 0 à 59. Le numéro par défaut est 1.
 - **Heures** Nombre d'heures de la période de location. La plage est de 0 à 22.
 - **Minutes** Nombre de minutes de la période de location. La plage est de 0 à 86399.
10. Pour configurer les adresses de routeur par défaut, cliquez sur le lien **adresses de routeur par défaut** et ajoutez jusqu'à huit adresses IP pour les routeurs par défaut, par ordre de préférence.
11. Pour configurer les adresses de serveur DNS, cliquez sur le lien **adresses de serveur DNS** et ajoutez jusqu'à huit adresses IP pour les serveurs DNS, par ordre de préférence.

12. Pour configurer les adresses des serveurs de noms NetBIOS, cliquez sur le lien **adresses des serveurs de noms NetBIOS** et ajoutez jusqu'à huit adresses IP pour les serveurs de noms NetBIOS, par ordre de préférence.
13. Dans le menu **NetBIOS Node type**, sélectionnez l'un des types de nœud NetBIOS suivants pour les clients DHCP :
 - **Diffusion de nœud b.**
 - **Nœud p poste à poste**
 - **Nœud M mixte**
 - **Hybride H-node**
14. Dans le champ **adresse du serveur suivant**, entrez l'adresse IP du serveur suivant qui doit être utilisé dans le processus de démarrage d'un client DHCP.
15. Dans le champ **Domain Name**, entrez le nom de domaine qui doit être utilisé dans le processus d'amorçage d'un client DHCP.
Le nom de domaine peut contenir jusqu'à 255 caractères.
16. Dans le champ **bootfile**, entrez le nom de l'image de démarrage par défaut qui doit être utilisée dans le processus de démarrage d'un client DHCP.
Le nom du fichier d'amorçage peut contenir jusqu'à 128 caractères.
17. Pour configurer les adresses de serveur NTP qui doivent être utilisées dans le processus de démarrage d'un client DHCP, cliquez sur le lien **serveur NTP** et ajoutez jusqu'à deux adresses IP pour les serveurs NTP, par ordre de préférence.
18. Cliquez sur le bouton **Add** (Ajouter).
La configuration du pool est ajoutée.
19. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Modifier un pool DHCP

Vous pouvez modifier un pool DHCP existant.

Pour modifier un pool DHCP :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.
4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **système > services > serveur DHCP > Configuration du pool DHCP**.
La page DHCP Pool Configuration s'affiche.
6. Dans le menu **Pool Name**, sélectionnez le pool.
7. Modifiez les paramètres en fonction de vos besoins.
Pour plus d'informations sur les paramètres, reportez-vous à la section [Créez un pool DHCP](#) à la page 178.
8. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimer un pool DHCP

Vous pouvez supprimer une règle de trafic dont vous n'avez plus besoin.

Pour supprimer un pool DHCP :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > services > serveur DHCP > informations sur les conflits DHCP**.

La page DHCP Pool Configuration s'affiche.

6. Dans le menu **Pool Name**, sélectionnez le pool.

7. Cliquez sur le bouton **Supprimer**.

Le pool est supprimé.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez les options de pool DHCP

Vous pouvez spécifier les informations à inclure dans le champ « options » d'un message DHCP envoyé par le commutateur.

Pour configurer les options de pool DHCP :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur principale à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > services > serveur DHCP > Options du pool DHCP** .

La page DHCP Pool Options s'affiche.

6. Dans le menu **Pool Name**, sélectionnez le nom du pool.

7. Dans le champ **Code d'option**, spécifiez le code d'option configuré pour le pool.

La plage est de 1 à 254. Pour plus d'informations sur les options et leur format, consultez les informations sur la RFC 2132 à l'adresse <https://tools.ietf.org/html/rfc2132>.

8. Dans le menu **type d'option**, sélectionnez l'un des types d'option suivants pour le pool :

- **ASCII** : Entrez les informations dans le champ **valeur de l'option** au format ASCII.
- **Hex** : Entrez les informations dans le champ **valeur de l'option** au format hexadécimal. Les formats possibles sont xx:xx et xxxx.xxxx.
- **IP Address** (Adresse IP). Dans le champ **valeur de l'option**, entrez une adresse IPv4.

9. Dans le champ **valeur de l'option**, spécifiez la valeur de l'option pour le pool en fonction de votre sélection à l'étape précédente.

10. Cliquez sur le bouton **Add** (Ajouter).

Le code d'option est ajouté pour le pool.

11. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Lier un pool DHCP à une classe et configurer la liaison

Si vous configurez des pools et des classes DHCP à utiliser avec un relais DHCP (voir [Relais DHCP](#) à la page 192), vous pouvez lier un pool à une ou plusieurs classes et configurer les liaisons.

Une configuration de liaison spécifie les plages d'adresses IP auxquelles la liaison s'applique, si une demande d'adresse DHCP est acceptée ou refusée, et, en option, le chemin d'accès au fichier d'amorçage qu'un client doit télécharger à partir d'un serveur TFTP du réseau (c'est ce que l'on appelle le code d'option 67).

Pour lier un pool DHCP à une classe et configurer la liaison :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > services > serveur DHCP > Configuration de liaison de classe DHCP**.

La page DHCP Class Binding Configuration s'affiche. La page affiche différentes sections.

6. Dans le menu **Pool Name**, sélectionnez le pool.
Les étapes suivantes s'appliquent à la section Configuration de liaison de classe DHCP.
7. Dans le champ **nom de classe**, sélectionnez la classe.
8. Dans les champs **plage IP de** et **plage IP à**, entrez les adresses IP de début et de fin auxquelles la liaison s'applique.
Si la liaison doit s'appliquer à toutes les adresses IP de la classe, entrez 0.0.0.0 dans chaque champ.
9. Dans le menu **refuser la location**, sélectionnez si la demande DHCP est acceptée :
 - FAUX La requête DHCP est acceptée. Les périphériques définis par les plages d'adresses IP peuvent recevoir des adresses IP du serveur DHCP.
 - VRAI La demande DHCP est refusée. Les périphériques définis par les plages d'adresses IP ne peuvent pas recevoir d'adresses IP du serveur DHCP.
10. Dans le champ **bootfile**, entrez éventuellement le chemin d'accès à un fichier d'amorçage sur un serveur TFTP du réseau.
Si la sélection dans le menu **refuser la location** est **FALSE**, les périphériques téléchargent et installent le fichier d'amorçage à partir du serveur TFTP. Le chemin du fichier peut contenir jusqu'à 128 caractères.
11. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
12. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Afficher les statistiques du serveur DHCP

Pour afficher les statistiques du serveur DHCP :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > services > serveur DHCP > statistiques du serveur DHCP**.

La page statistiques du serveur DHCP s'affiche.

6. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).
7. Pour effacer les statistiques, cliquez sur le bouton **Effacer**.
8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 39 : Informations statistiques du serveur DHCP

Champ	Description
Détails de la liaison	
Liaisons automatiques	Nombre de liaisons automatiques sur le serveur DHCP
Liaisons expirées	Nombre de liaisons expirées sur le serveur DHCP
Messages mal formés	Nombre de messages mal formés sur le serveur DHCP
Message reçu	
DHCPDISCOVER	Nombre de messages DHCPDISCOVER reçus par le serveur DHCP
DHCPREQUEST	Nombre de messages DHCPREQUEST reçus par le serveur DHCP
DHCPDECLINE	Nombre de messages DHCPDECLINE reçus par le serveur DHCP
DHCPRELEASE	Nombre de messages DHCPRELEASE reçus par le serveur DHCP
DHCPINFORM	Nombre de messages DHCPINFORM reçus par le serveur DHCP
Message envoyé	
DHCPOFFER	Nombre de messages DHCPOFFER envoyés par le serveur DHCP

Table 39 : Informations statistiques du serveur DHCP (A continué)

Champ	Description
DHCPACK	Nombre de messages DHCPACK envoyés par le serveur DHCP
DHCPNAK	Nombre de messages DHCPNAK envoyés par le serveur DHCP
Paquets DE DÉCOUVERTE DHCP refusés bail	Nombre de messages DE DÉCOUVERTE DHCP refusés par le serveur DHCP

Afficher les liaisons DHCP

Pour afficher les liaisons DHCP :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.
4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **système > services > serveur DHCP > informations sur les liaisons DHCP**.

La page informations sur les liaisons DHCP s'affiche. Le tableau affiche des informations sur toutes les liaisons.

6. Pour rechercher une liaison avec un conflit d'adresse IP, entrez l'adresse IP dans le champ **Rechercher une adresse IP de conflit** et cliquez sur le bouton **aller**.

Des informations sur la reliure s'affichent.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 40 : Informations sur les liaisons DHCP

Champ	Description
Adresse IP	Adresse IP du client
Nom du pool	Nom du pool dont fait partie le client
Adresse matérielle	Adresse matérielle du client
Temps de location restant	Le temps de location restant en jours, heures et minutes (format jj:hh:mm)
Type	Le type de reliure (dynamique ou manuelle)

Supprimez une ou toutes les liaisons DHCP dynamiques

Pour supprimer une ou toutes les liaisons DHCP dynamiques :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > services > serveur DHCP > informations sur les liaisons DHCP**.

La page informations sur les liaisons DHCP s'affiche.

6. Sélectionnez l'une des cases d'option suivantes :

- **Toutes les liaisons dynamiques** : Toutes les liaisons dynamiques doivent être effacées.
- **Liaison dynamique spécifique** : Dans le champ, spécifiez l'adresse IP de la liaison dynamique qui doit être effacée.

7. Cliquez sur le bouton **Clear** (Effacer).

La ou les liaisons sélectionnées sont supprimées.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Afficher les liaisons avec conflits DHCP

Vous pouvez afficher des informations sur les périphériques présentant des conflits d'adresses IP. Un conflit peut se produire lorsque la même adresse IP est attribuée à deux périphériques ou plus du réseau.

Pour afficher les liaisons DHCP avec conflits :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > services > serveur DHCP > informations sur les conflits DHCP**.

La page informations sur les conflits DHCP s'affiche. Le tableau affiche des informations sur toutes les liaisons en conflit.

6. Pour rechercher une liaison avec un conflit d'adresse IP, entrez l'adresse IP dans le champ **Rechercher une adresse IP de conflit** et cliquez sur le bouton **aller**.

Des informations sur la reliure s'affichent.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 41 : Informations sur les conflits DHCP

Champ	Description
Adresse IP	Adresse IP du client DHCP.
Adresse matérielle	Adresse matérielle du client DHCP.
Méthode de détection	Méthode avec laquelle l'adresse IP du client DHCP a été détectée sur le serveur DHCP.
Temps de détection	Heure à laquelle le conflit a été détecté au format jours;heures;minutes;secondes depuis le dernier redémarrage du commutateur.

Supprimez une ou toutes les liaisons DHCP présentant des conflits

Pour supprimer une ou toutes les liaisons DHCP en conflit :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.
4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **système > services > serveur DHCP > informations sur les conflits DHCP**.
La page informations sur les conflits DHCP s'affiche.
6. Sélectionnez l'une des cases d'option suivantes :
 - **Tous les conflits d'adresses** : Toutes les liaisons avec des conflits d'adresse IP doivent être effacées.
 - **Conflit d'adresse spécifique** : Dans le champ, spécifiez l'adresse IP de la liaison avec un conflit qui doit être effacé.
7. Cliquez sur le bouton **Clear** (Effacer).

La ou les liaisons sélectionnées sont supprimées.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Relais DHCP

Le commutateur peut fonctionner comme un périphérique de couche 3 dans lequel informatique relaie les messages entre les clients DHCP et les serveurs DHCP situés dans un sous-réseau IP différent. Nous désignons le commutateur comme un relais DHCP de couche 3, ou simplement un relais DHCP, par opposition à un relais DHCP de couche 2, qui est une fonction différente (voir [Relais DHCP de couche 2](#) à la page 197).

Configurez les paramètres de relais DHCP globaux et affichez les statistiques de relais

Vous pouvez activer l'agent de relais DHCP de couche 3 sur le commutateur et laisser le commutateur relayer les messages DHCP entre les clients DHCP et les serveurs DHCP situés dans un sous-réseau IP différent.

Pour configurer les paramètres de relais DHCP globaux et afficher les statistiques de relais :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > services > Relais DHCP**.

La page Relais DHCP s'affiche.

6. Dans le champ **nombre maximal de sauts**, entrez le nombre maximal de sauts qu'une requête client peut prendre avant d'être rejetée.

La plage est de 1 à 16. Le numéro par défaut est 4.

7. Sélectionnez le bouton radio mode Admin **désactiver** ou **Activer** pour désactiver ou activer le relais DHCP sur le commutateur.

8. Dans le champ **temps d'attente minimum**, entrez le temps minimum en secondes que le relais DHCP doit attendre avant de transférer les demandes.

L'heure est comparée à l'horodatage dans les paquets de requête DHCP du client, qui représente le temps écoulé depuis la mise sous tension du client. Les paquets sont transmis uniquement lorsque l'horodatage dépasse le temps d'attente minimum. La plage est de 0 à 100.

9. Sélectionnez l'un des boutons radio mode option ID circuit suivants :

- Désactiver : Les options d'agent de relais ne sont pas ajoutées aux demandes avant qu'elles ne soient transférées au serveur et ne sont pas supprimées des réponses avant qu'elles ne soient transférées aux clients.
- Activer. Les options d'agent de relais sont ajoutées aux demandes avant qu'elles ne soient transmises au serveur et supprimées des réponses avant qu'elles ne soient transmises aux clients.
- Aucun : L'option ID circuit n'est pas configurée. Cette sélection est en fait identique à la sélection désactiver.

10. Sélectionnez l'un des boutons radio Server Override mode suivants :

- Désactiver : Les sous-options 5 et 11 ne sont pas ajoutées à l'option 82 du paquet DHCP entrant.

La sous-option 5 spécifie le sous-réseau IP à partir duquel le serveur DHCP doit attribuer des adresses IP.

La sous-option 11 spécifie que l'ID du serveur peut être remplacé par un nouvel ID.

- Activer. Les sous-options 5 et 11 sont ajoutées à l'option 82 d'un paquet DHCP entrant.

11. Dans le menu **source interface**, sélectionnez une interface ou VLAN.

Il s'agit de l'interface ou VLAN connectée aux serveurs DHCP situés dans un sous-réseau IP différent.

12. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

13. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

14. Pour actualiser les informations de la page, cliquez sur le bouton Actualiser.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 42 : Informations sur l'état du relais DHCP

Champ	Description
Messages client DHCP reçus	Nombre de requêtes DHCP reçues des clients.
Messages client DHCP relayés	Nombre de requêtes DHCP transmises aux serveurs.
Messages du serveur DHCP reçus	Nombre de messages de serveur DHCP reçus des serveurs.
Messages du serveur DHCP relayés	Nombre de messages de serveur DHCP transférés depuis les serveurs.
Messages client UDP reçus	Nombre de requêtes UDP reçues des clients. Il s'agit de messages transmis via UDP à partir d'un client DHCP (externe au commutateur) et détectés par le relais DHCP sur le commutateur.
Messages client UDP relayés	Nombre de requêtes UDP transmises aux serveurs. Ce sont des messages qui sont relayés via UDP à un serveur DHCP (externe au commutateur) et qui sont détectés par le relais DHCP sur le commutateur.
Le nombre de sauts de messages DHCP a dépassé le nombre maximum de	Nombre de messages client DHCP reçus pour lesquels le nombre de sauts dépasse le nombre maximal de sauts configuré. Ces messages ne sont pas relayés.
Message DHCP avec le champ secondes inférieur à min	Nombre de messages client DHCP reçus pour lesquels le temps d'attente minimum est inférieur à la valeur minimum configurée. Ces messages ne sont pas relayés.
Message DHCP avec giaddr défini sur l'adresse locale	Nombre de messages client DHCP reçus pour lesquels l'adresse de passerelle (giaddr) est déjà définie sur une adresse IP configurée sur l'une des adresses IP de l'agent relais. Dans ce cas, un autre périphérique pourrait tenter d'usurper l'adresse de l'agent relais. Ces messages ne sont pas relayés.

Table 42 : Informations sur l'état du relais DHCP (A continué)

Champ	Description
Paquets avec TTL expiré	Le nombre de paquets reçus avec un temps de vie de 0 seconde ou 1 seconde. Ces paquets ne sont pas relayés.
Paquets correspondant à une entrée de suppression	Nombre de paquets ignorés par l'agent relais car les paquets correspondent à une entrée de relais de suppression.

Configurez une interface de relais DHCP

Vous pouvez activer l'agent de relais DHCP de couche 3 sur une interface de routage et laisser l'interface relayer les messages DHCP entre les clients DHCP et les serveurs DHCP situés dans un sous-réseau IP différent.

Pour configurer une interface de relais DHCP :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > services > Relais DHCP**.

La page Relais DHCP s'affiche.

6. Faites défiler vers le bas jusqu'à la section du relais DHCP inférieur en bas de la page.

Si aucune interface de routage n'est configurée sur le commutateur, le tableau de configuration du relais DHCP ne s'affiche pas sur la page.

7. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :

- **1 ou ID d'unité pour un commutateur empilé :**

- 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
- **ID d'unité pour un commutateur empilé :** Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.

- VLAN Seuls les VLAN sont affichés.

- **Tous:** Les interfaces physiques et les VLAN sont affichés, ou pour une pile de commutateurs, les interfaces physiques et les VLAN de tous les commutateurs sont affichés.

8. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :

- Pour afficher ou effacer les statistiques d'une seule interface, cochez la case associée à l'interface ou saisissez le numéro de l'interface dans le champ **aller à l'interface** et cliquez sur le bouton **aller**.
- Pour configurer plusieurs interfaces avec les mêmes paramètres, cochez la case associée à chaque interface.
- Pour configurer toutes les interfaces avec les mêmes paramètres, cochez la case dans la ligne d'en-tête.

9. Sélectionnez l'un des boutons radio Server Override mode suivants :

- Désactiver : Les sous-options 5 et 11 ne sont pas ajoutées à l'option 82 du paquet DHCP entrant.

La sous-option 5 spécifie le sous-réseau IP à partir duquel le serveur DHCP doit attribuer des adresses IP.

La sous-option 11 spécifie que l'ID du serveur peut être remplacé par un nouvel ID.

- Activer. Les sous-options 5 et 11 sont ajoutées à l'option 82 d'un paquet DHCP entrant.

10. Dans le menu **source interface**, sélectionnez une interface ou VLAN.

Il s'agit de l'interface ou VLAN connectée aux serveurs DHCP situés dans un sous-réseau IP différent.

11. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

12. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Relais DHCP de couche 2

Si vous activez et configurez un agent de relais DHCP sur le commutateur, certains périphériques de couche 2 (L2) n'ont pas besoin de se connecter à un serveur DHCP sur le réseau physique. Un agent de relais remplit automatiquement le champ adresse IP de la passerelle (giaddr) et ajoute l'option informations sur l'agent de relais aux messages DHCP. Un serveur DHCP utilise cette option pour les adresses IP et d'autres stratégies d'attribution. Un agent de relais DHCP est généralement un périphérique sensible au routage IP, également appelé agent de relais de couche 3. Dans certaines configurations réseau, les périphériques L2 doivent ajouter l'option Relay agent information car ils sont plus proches des hôtes finaux.

Un périphérique L2 peut fonctionner comme un pont uniquement pour un réseau et peut ne pas inclure d'adresse IPv4 sur le réseau. Si un périphérique L2 n'a pas d'adresse source IPv4, il ne peut pas relayer les paquets directement à un serveur DHCP situé sur un autre réseau. Dans ce cas, le périphérique L2 peut ajouter l'option Relay agent information et diffuser le message DHCP.

Configurez les paramètres globaux du relais DHCP L2

Pour configurer les paramètres globaux du relais DHCP L2 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > services > Relais DHCP L2 > Configuration globale du Relais DHCP L2**.

La page DHCP L2 Relay Global Configuration s'affiche.

6. Sélectionnez le bouton radio mode Admin **désactiver** ou **Activer** pour désactiver ou activer le relais DHCP L2 sur le commutateur.

La valeur par défaut est désactiver.

7. Dans la section Configuration du relais DHCP L2 VLAN, configurez les paramètres suivants :

- **Identifiant VLAN** : ID du VLAN déjà configuré sur le commutateur.
Vous ne pouvez pas utiliser cette page pour ajouter un VLAN. Pour plus d'informations sur l'ajout de VLAN, reportez-vous à la section [VLAN](#) à la page 310.
- **Mode Admin Activer ou désactiver le relais DHCP L2 sur le VLAN.**
- **Mode ID circuit** : Activez ou désactivez la sous-option ID circuit de DHCP option-82.
- **Chaîne ID distante** : Spécifiez l'ID distant si l'option ID distant est activée.

8. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez une interface de relais DHCP L2

Vous pouvez configurer un relais DHCP L2 sur une interface.

Pour configurer l'interface de relais L2 DHCP :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > services > Relais DHCPL2 > Configuration de l'interface de relais DHCP L2**.

La fenêtre Configuration de l'interface de relais L2 DHCP s'affiche.

6. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :

- **1 ou ID d'unité pour un commutateur empilé :**

- 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
 - **ID d'unité pour un commutateur empilé** : Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
 - LAG Seuls les LAG sont affichés.
 - **Tous**: Les interfaces physiques et les LAG sont affichés, ou pour une pile de commutateurs, les interfaces physiques de tous les commutateurs de la pile et les LAG sont affichés.
7. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :
- Pour afficher ou effacer les statistiques d'une seule interface, cochez la case associée à l'interface ou saisissez le numéro de l'interface dans le champ **aller à l'interface** et cliquez sur le bouton **aller**.
 - Pour configurer plusieurs interfaces avec les mêmes paramètres, cochez la case associée à chaque interface.
 - Pour configurer toutes les interfaces avec les mêmes paramètres, cochez la case dans la ligne d'en-tête.
8. Dans le menu **Admin mode**, sélectionnez pour activer ou désactiver le relais DHCP L2 sur l'interface.
- La valeur par défaut est désactiver.
9. Dans le menu **82 option Trust mode**, sélectionnez pour activer ou désactiver l'interface en tant qu'interface approuvée pour l'option Relay agent information (informations sur l'agent de relais) (option 82).
10. Dans le menu **No 82 option Trust mode**, sélectionnez la manière dont l'interface traite les paquets reçus sans l'option 82 :
- Abandonné L'interface supprime les paquets reçus sans l'option 82.
 - Mettre à jour L'interface ajoute l'option 82 aux paquets reçus sans l'option 82.
- Les paramètres de ce menu ne peuvent être activés que si vous sélectionnez **Activer** dans le menu **82 option mode confiance**.
11. Cliquez sur le bouton **Apply** (Appliquer).
- Les paramètres sont enregistrés.
12. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Affiche les statistiques de l'interface de relais L2 DHCP

Pour afficher les statistiques de l'interface de relais L2 DHCP :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > services > Relais DHCPL2 > statistiques de l'interface de relais DHCP L2**.

La page statistiques de l'interface de relais DHCP L2 s'affiche.

6. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :

- **1 ou ID d'unité pour un commutateur empilé :**

- 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
 - **ID d'unité pour un commutateur empilé** : Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
 - LAG Seuls les LAG sont affichés.
 - VLAN Seuls les VLAN sont affichés.
 - **Tous**: Les interfaces physiques, les LAG et les VLAN sont affichés, ou pour une pile de commutateurs, les interfaces physiques de tous les commutateurs de la pile, les LAG et les VLAN sont affichés.
7. Pour actualiser les informations de la page, cliquez sur **le** bouton Actualiser.
- Le tableau suivant décrit les champs en lecture seule de la page.

Table 43 : Informations statistiques sur l'interface de relais L2 DHCP

Champ	Description
Interface	Interface à partir de laquelle le message DHCP est reçu
UntrustedServerMsgsWithOpt82	Nombre de messages DHCP avec l'option 82 reçus d'un serveur non approuvé
UntrustedClientMsgsWithOpt82	Nombre de messages DHCP avec l'option 82 reçus d'un client non approuvé
TrustedServerMsgsWithoutOpt82	Nombre de messages DHCP sans option 82 reçus d'un serveur approuvé
TrustedClientMsgsWithoutOpt82	Nombre de messages DHCP sans option 82 reçus d'un client de confiance

Relais UDP

Vous pouvez activer le commutateur pour qu'il fonctionne comme un relais UDP, ce qui permet au commutateur de transférer des paquets de diffusion UDP (User Datagram Protocol) d'un routeur vers une adresse IP sur un sous-réseau local ou non local.

Configurez les paramètres de relais UDP globaux et ajoutez un relais UDP

Pour configurer les paramètres de relais UDP globaux et ajouter un relais UDP :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > services > Relais UDP > Configuration globale du Relais UDP**.

La page Configuration globale du relais UDP s'affiche.

6. Sélectionnez le bouton radio mode Admin **désactiver** ou **Activer** pour désactiver ou activer le relais UDP sur le commutateur.

La valeur par défaut est désactiver.

7. Dans la section Configuration globale du relais UDP, configurez les paramètres suivants :

- **Server Address** (Adresse du serveur). Entrez l'adresse IPv4 du serveur relais UDP.
- **Port UDP** : Sélectionnez l'un des types de ports de destination UDP suivants :
 - AUTRE Le champ **autre valeur du port UDP** devient disponible pour vous permettre de saisir un numéro de port UDP personnalisé.
 - DHCP Paquets DHCP de relais (port UDP 67).
 - Domaine : Paquets DNS de relais (port UDP 53).
 - **isakmp** : Paquets ISAKMP de relais (port UDP 500).

- **mobile-ip** : Relais de paquets IP mobile (port UDP 434)
 - **Nameserver** (Serveur de nom) - Relais IEN-116 Name Service (port UDP 42) paquets
 - **netbios-dgm** : Paquets Relais NetBIOS Datagram Server (port UDP 138)
 - **netbios-ns** : Paquets de serveur de noms NetBIOS relais (port UDP 137)
 - **ntp** : Paquets de protocole de temps de réseau de relais (port UDP 123).
 - **pim-auto-rp** : Relais PIM auto RP (port UDP 496) paquets.
 - RIP Paquets RIP (Relay Routing image Protocol) (port UDP 520)
 - TACACS+ Paquet TACACS de relais (port UDP 49)
 - TFTP Paquets TFTP de relais (port UDP 69)
 - Horaire : Paquets de service de temps de relais (port UDP 37)
 - **Port UDP autre valeur** : Si vous sélectionnez **autre** dans le menu **Port UDP**, entrez un numéro de port UDP personnalisé compris entre 0 et 65535.
8. Cliquez sur le bouton **Add** (Ajouter).
Le relais UDP est ajouté.
Le champ nombre d'appels affiche le nombre de paquets UDP détectés sur le port UDP du relais UDP.
9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Modifier la configuration d'un relais UDP

Pour modifier la configuration d'un relais UDP :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > services > Relais UDP > Configuration globale du Relais UDP**.

La page Configuration globale du relais UDP s'affiche.

6. Dans la section Configuration globale du relais UDP, cochez la case correspondant à la configuration du relais UDP.

7. Modifiez les paramètres en fonction de vos besoins.

Pour plus d'informations sur les paramètres, reportez-vous à la section .

8. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimer une configuration de relais UDP

Pour supprimer une configuration de relais UDP :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **système > services > Relais UDP > Configuration globale du Relais UDP**.
La page Configuration globale du relais UDP s'affiche.
6. Dans la section Configuration globale du relais UDP, cochez la case correspondant à la configuration du relais UDP.
7. Cliquez sur le bouton **Supprimer**.
La configuration du commutateur UDP est supprimée.
8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Ajoutez une configuration d'interface UDP

Pour ajouter une configuration d'interface de relais UDP :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > services > Relais UDP > Configuration de l'interface de relais UDP**.

La page Configuration de l'interface de relais UDP s'affiche.

6. Dans le menu **interface**, sélectionnez l'interface ou le VLAN pour lequel vous ajoutez la configuration UDP.
7. Dans le champ **adresse du serveur**, entrez l'adresse IPv4 du serveur relais UDP.
8. Dans le menu **Port UDP**, sélectionnez l'un des types de ports de destination UDP suivants :

- **AUTRE** Le champ **autre valeur du port UDP** devient disponible pour vous permettre de saisir un numéro de port UDP personnalisé.
- **DHCP** Paquets DHCP de relais (port UDP 67).
- **Domaine** : Paquets DNS de relais (port UDP 53).
- **isakmp** : Paquets ISAKMP de relais (port UDP 500).
- **mobile-ip** : Relais de paquets IP mobile (port UDP 434)
- **Nameserver** (Serveur de nom) - Relais IEN-116 Name Service (port UDP 42) paquets
- **netbios-dgm** : Paquets Relais NetBIOS Datagram Server (port UDP 138)
- **netbios-ns** : Paquets de serveur de noms NetBIOS relais (port UDP 137)
- **ntp** : Paquets de protocole de temps de réseau de relais (port UDP 123).
- **pim-auto-rp** : Relais PIM auto RP (port UDP 496) paquets.
- **RIP** Paquets RIP (Relay Routing image Protocol) (port UDP 520)
- **TACACS+** Paquet TACACS de relais (port UDP 49)

- TFTP Paquets TFTP de relais (port UDP 69)
 - Horaire : Paquets de service de temps de relais (port UDP 37)
9. Si vous sélectionnez **autre** dans le menu **Port UDP**, entrez un numéro de port UDP personnalisé dans le champ **autre valeur du port UDP** .
- Le numéro de port doit être compris entre 0 et 65535.
10. Dans le menu **rejeter**, sélectionnez si les paquets qui correspondent à la condition sont abandonnés :
- Activer. Les paquets sont abandonnés. Cette sélection ne fonctionne que si vous entrez 0.0.0.0 comme adresse IP du serveur.
 - Abandonner Les paquets ne sont pas abandonnés. Cette sélection fonctionne si l'adresse IP du serveur n'est pas 0,0.0,0.
11. Cliquez sur le bouton **Add** (Ajouter).
- La configuration de l'interface UDP est ajoutée.
- Le champ nombre d'accès affiche le nombre de paquets UDP détectés sur l'interface UDP.
12. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Modifier une configuration d'interface UDP

Pour modifier la configuration d'un commutateur UDP :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > services > Relais UDP > Configuration de l'interface de relais UDP**.

La page Configuration de l'interface de relais UDP s'affiche.

6. Dans le menu **interface**, sélectionnez l'interface ou VLAN.

7. Modifiez les paramètres en fonction de vos besoins.

Pour plus d'informations sur les paramètres, reportez-vous à la section .

8. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimer une interface UDP

Pour supprimer une interface UDP :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > services > Relais UDP > Configuration de l'interface de relais UDP**.

La page Configuration de l'interface de relais UDP s'affiche.

6. Dans le menu **interface**, sélectionnez l'interface ou VLAN.

7. Cliquez sur le bouton **Supprimer**.

L'interface UDP est supprimée.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Serveur DHCPv6

Vous pouvez configurer les paramètres d'un serveur DHCPv6, de pools DHCPv6, de délégation de préfixe DHCPv6, d'interfaces DHCPv6 et de liaisons DHCPv6. Vous pouvez également afficher les statistiques DHCPv6.

Activez le serveur DHCPv6

Par défaut, le serveur DHCPv6 est désactivé. Vous pouvez activer informatique pour que le commutateur puisse attribuer des informations de configuration réseau aux clients IPv6.

Pour activer le serveur DHCPv6 sur le commutateur :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > services > serveur DHCPv6 > Configuration du serveur DHCPv6**.

La page Configuration du serveur SNTP s'affiche.

6. Sélectionnez le bouton radio **Activer** le mode Admin.

La valeur par défaut est désactiver.

7. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

Le champ DUID du serveur DHCPv6 affiche l'identifiant unique DHCP (DUID) du serveur DHCPv6.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Gérer les pools DHCPv6

Un pool DHCPv6 fournit des informations de configuration réseau qui sont disponibles pour les clients DHCPv6 qui demandent de telles informations. Vous pouvez ajouter, modifier et supprimer des pools DHCPv6.

Créez un pool DHCPv6

Un pool DHCPv6 fournit des informations de configuration réseau qui sont disponibles pour les clients DHCPv6 qui demandent de telles informations.

Pour créer un pool DHCPv6 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > services > serveur DHCPv6 > Configuration du pool DHCPv6**.

La page Configuration du pool DHCPv6 s'affiche.

6. Dans le menu **Pool Name (nom du pool)**, sélectionnez **Create(créer)**.

7. Dans le champ **Pool Name**, saisissez un nom identifiant le pool de serveurs DHCPv6.
Le nom peut contenir jusqu'à 31 caractères.
8. Cliquez sur le lien **adresses du serveur DNS** et spécifiez la liste des adresses de routeur IPv6 par défaut pour le pool.
Vous pouvez spécifier jusqu'à huit adresses de routeur par défaut par ordre de préférence.
9. Cliquez sur le lien **nom de domaine** et spécifiez la liste des noms de domaine IPv6 pour le pool.
Un nom de domaine peut contenir jusqu'à 255 caractères alphanumériques.
10. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
11. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Modifier un pool DHCPv6

Vous pouvez modifier un pool DHCPv6 existant.

Pour modifier un pool DHCPv6 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **système > services > serveur DHCPv6 > Configuration du pool DHCPv6**.
La page Configuration du pool DHCPv6 s'affiche.
6. Dans le menu **Pool Name**, sélectionnez le nom du pool.
(Vous ne pouvez pas modifier le nom d'utilisateur.)
7. Cliquez sur le lien **adresses du serveur DNS** et modifiez la liste des adresses de routeur IPv6 par défaut pour le pool.
Vous pouvez spécifier jusqu'à huit adresses de routeur par défaut par ordre de préférence.
8. Cliquez sur le lien **nom de domaine** et modifiez la liste des noms de domaine IPv6 pour le pool.
Un nom de domaine peut contenir jusqu'à 255 caractères alphanumériques.
9. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimer un pool DHCPv6

Vous pouvez supprimer un VLAN DHCPv6 de base dont vous n'avez plus besoin.

Pour supprimer un pool DHCPv6 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > services > serveur DHCPv6 > Configuration du pool DHCPv6**.

La page Configuration du pool DHCPv6 s'affiche.

6. Dans le menu **Pool Name**, sélectionnez le nom du pool.

7. Cliquez sur le bouton **Supprimer**.

Le pool est supprimé.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Gérer la délégation du préfixe DHCPv6 pour les pools

Une configuration de délégation de préfixe fournit un préfixe IPv6 et une longueur de préfixe à un pool DHCPv6 qui fournit des informations de configuration réseau aux clients DHCPv6 qui demandent de telles informations.

Un client DHCPv6 peut demander plusieurs préfixes IPv6 et peut également demander des préfixes IPv6 spécifiques. Si un pool DHCPv6 contient le préfixe spécifique demandé par un client DHCPv6, le préfixe est délégué au client. Sinon, le premier préfixe IPv6 disponible dans un pool est délégué au client.

Créez une configuration de délégation de préfixe DHCPv6 pour un pool

Vous pouvez créer une configuration de délégation de préfixe DHCPv6 pour un pool.

Pour créer une configuration de délégation de préfixe DHCPv6 pour un pool :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > services > serveur DHCPv6 > Configuration de délégation de préfixe DHCPv6**.

La page Configuration de la délégation de préfixe DHCPv6 s'affiche.

6. Dans le menu **Pool Name**, sélectionnez un pool.
7. Dans le champ **préfixe**, spécifiez le préfixe IPv6.
8. Dans le champ **longueur du préfixe**, spécifiez la longueur associée au préfixe IPv6.
9. Dans le champ **DUID**, spécifiez l'identificateur unique DHCP (DUID) associé au préfixe IPv6.

❗ Remarque: Le DUID et le nom du client sont utilisés uniquement si un périphérique demande un préfixe. De cette façon, le périphérique reçoit un préfixe IPv6 au lieu d'une adresse IPv6 spécifique. Si vous attribuez une adresse IPv6 spécifique au périphérique, vous pouvez laisser les champs DUID et nom du client vides.

10. Dans le champ **nom du client**, entrez un nom de client associé au préfixe IPv6.

Le nom, utile pour la journalisation ou le traçage, peut comporter jusqu'à 31 caractères.

11. Dans le champ **durée de vie valide**, entrez la durée en secondes après laquelle le préfixe IPv6 expire.

Saisissez une valeur comprise entre 0 et 4294967295.

12. Dans le champ **durée de vie préférée**, entrez la durée préférée en secondes après laquelle le préfixe IPv6 expire.

Saisissez une valeur comprise entre 0 et 4294967295.

13. Cliquez sur le bouton **Add** (Ajouter).

La configuration de délégation de préfixe est ajoutée pour le pool sélectionné.

14. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Modifier une configuration de délégation de préfixe DHCPv6 pour un pool

Vous pouvez modifier une configuration de délégation de préfixe DHCPv6 existante.

Pour modifier une configuration de délégation de préfixe DHCPv6 pour un pool :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **système > services > serveur DHCPv6 > Configuration de délégation de préfixe DHCPv6** .
La page Configuration de la délégation de préfixe DHCPv6 s'affiche.
6. Dans le menu **Pool Name**, sélectionnez le pool.
7. Modifiez les paramètres en fonction de vos besoins.
Pour plus d'informations sur les paramètres, reportez-vous à la section .
8. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimez une configuration de délégation de préfixe DHCPv6 pour un pool

Vous pouvez supprimer une configuration de délégation de préfixe DHCPv6 existante dont vous n'avez plus besoin.

Pour supprimer une configuration de délégation de préfixe DHCPv6 pour un pool :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > services > serveur DHCPv6 > Configuration de délégation de préfixe DHCPv6**.

La page Configuration de la délégation de préfixe DHCPv6 s'affiche.

6. Dans le menu **Pool Name**, sélectionnez le pool.

7. Cliquez sur le bouton **Supprimer**.

La configuration de délégation de préfixe est supprimée.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez les paramètres cos d'une interface .

Vous pouvez configurer les paramètres DHCPv6 d'une interface afin que celle-ci puisse fournir des services DHCPv6 aux périphériques connectés.

Pour configurer les paramètres DHCPv6 d'une interface :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > services > serveur DHCPv6 > Configuration de l'interface DHCPv6**.

La page Configuration de l'interface DHCPv6 s'affiche.

6. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :

- **1 ou ID d'unité pour un commutateur empilé :**
 - 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
 - **ID d'unité pour un commutateur empilé :** Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
- **VLAN** Seuls les VLAN sont affichés.
- **Tous:** Les interfaces physiques et les VLAN sont affichés, ou pour une pile de commutateurs, les interfaces physiques et les VLAN de tous les commutateurs sont affichés.

7. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :

- Pour afficher ou effacer les statistiques d'une seule interface, cochez la case associée à l'interface ou saisissez le numéro de l'interface dans le champ **aller à l'interface** et cliquez sur le bouton **aller**.
- Pour configurer plusieurs interfaces avec les mêmes paramètres, cochez la case associée à chaque interface.
- Pour configurer toutes les interfaces avec les mêmes paramètres, cochez la case dans la ligne d'en-tête.

8. Dans le menu **mode Admin**, sélectionnez pour activer ou désactiver le mode serveur DHCPv6 sur l'interface.

❗ **Remarque:** Les fonctions serveur DHCPv6 et relais DHCPv6 sont mutuellement exclusives. Pour plus d'informations sur la configuration d'une interface en tant que relais DHCPv6, reportez-vous à la section Interface de relais DHCPv6 à la page 227.

9. Dans le champ **Pool Name**, sélectionnez un pool DHCPv6.
Pour plus d'informations, consultez la section Gérer les pools DHCPv6 à la page 212.
10. Dans le menu **Rapid Commit**, sélectionnez pour activer ou désactiver un échange abrégé entre le périphérique qui demande des informations IPv6 et le serveur DHCPv6.
Ce paramètre est facultatif.
11. Dans le champ **préférence**, spécifiez la valeur de préférence qu'un périphérique peut utiliser pour déterminer la préférence de cette interface par rapport aux autres serveurs DHCPv6.
Vous pouvez entrer une valeur comprise entre 0 et 4294967295. Le numéro par défaut est 0.
12. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
13. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Afficher les liaisons DHCPv6

Une fois qu'un client a acquis des informations de configuration IPv6 à partir d'un serveur DHCPv6, le serveur ajoute une entrée à la table de liaisons DHCPv6.

Pour afficher les informations sur les liaisons DHCPv6 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **système > services > serveur DHCPv6 > informations sur les liaisons DHCPv6** .
La page informations sur les liaisons DHCPv6 s'affiche.
6. Pour rechercher une liaison, entrez l'adresse IPv6 dans le champ **Rechercher l'adresse IP de liaison** et cliquez sur le bouton **aller**.
Des informations sur la reliure s'affichent.
7. Le tableau suivant décrit les champs en lecture seule de la page.
8. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).
Le tableau suivant décrit les champs en lecture seule de la page.

Table 44 : Informations de liaison DHCPv6

Champ	Description
Adresse du client	Adresse IPv6 du client associé à la liaison.
Interface client	Numéro de l'interface sur laquelle la liaison client s'est produite.
DUID de client	Identificateur unique DHCPv6 (DUID) du client. Le DUID est une combinaison de l'adresse matérielle du client et de l'identifiant du client.
Préfixe :	Adresse IPv6 du préfixe délégué associé à cette liaison.
Longueur de préfixe	Longueur du masque IPv6 pour le préfixe délégué associé à cette liaison.
Type de préfixe	Type de préfixe IPv6 associé à cette liaison.
Heure d'expiration	Nombre de secondes avant expiration du préfixe associé à une liaison.

Table 44 : Informations de liaison DHCPv6 (A continué)

Champ	Description
Durée de vie valide	Durée maximale en secondes pendant laquelle le client est autorisé à utiliser le préfixe.
Préférez la vie	Durée préférée en secondes pendant laquelle le client est autorisé à utiliser le préfixe.

Afficher les statistiques du serveur DHCPv6

Vous pouvez afficher les statistiques du serveur DHCPv6, y compris les informations sur les messages DHCPv6 envoyés, reçus et supprimés globalement et sur chaque interface.

Pour afficher les statistiques du serveur DHCPv6 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > services > serveur DHCPv6 > statistiques du serveur DHCPv6**.

La page statistiques du serveur DHCPv6 s'affiche.

6. Effectuez l'une des opérations suivantes :

- **Afficher les statistiques pour une interface** : Dans le menu interface, sélectionnez l'interface.
- **Afficher les statistiques pour toutes les interfaces** : Dans le menu interface, sélectionnez **tout**.

7. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

Le tableau suivant décrit les champs en lecture seule de la page.

Table 45 : Informations statistiques sur le serveur DHCPv6

Champ	Description
Messages reçus	
Total des paquets DHCPv6 reçus	Nombre de messages de gestion reçus. Les messages DHCPv6 envoyés d'un client DHCP v6 à un serveur DHCP v6 incluent les messages solliciter, demander, confirmer, renouveler, relier, libérer, refuser et les messages de demande d'informations. En outre, un agent de relais DHCP v6 peut transférer des messages de transfert de relais à un serveur DHCP v6.
DHCPv6 solliciter les paquets reçus	Le nombre de messages de sollicitation DHCPv6 reçus. Ce type de message est envoyé par un client pour localiser les serveurs DHCPv6.
Paquets de requête DHCPv6 reçus	Nombre de demandes reçues.
DHCPv6 confirmer la réception des paquets	Le nombre de messages de confirmation DHCPv6 reçus. Ce type de message est envoyé par un client à tous les serveurs DHCPv6 pour déterminer si sa configuration est valide pour la liaison connectée.
DHCPv6 renouvellement des paquets reçus	Nombre de messages de renouvellement DHCPv6 reçus. Ce type de message est envoyé par un client pour étendre et mettre à jour les informations de configuration fournies par le serveur DHCPv6.
Paquets de reliaison DHCPv6 reçus	Nombre de messages de reliaison DHCPv6 reçus. Ce type de message est envoyé par un client à n'importe quel serveur DHCPv6 lorsque informatique ne reçoit pas de réponse à un message de renouvellement.
Paquets de version DHCPv6 reçus	Nombre de messages de version DHCPv6 reçus. Ce type de message est envoyé par un client pour indiquer que informatique n'a plus besoin de l'adresse attribuée.
Paquets de refus DHCPv6 reçus	Nombre de messages de refus DHCPv6 reçus. Ce type de message est envoyé par un client au serveur DHCPv6 pour indiquer qu'une adresse attribuée est déjà utilisée sur la liaison.
DHCPv6 informez les paquets reçus	Nombre de messages de demande d'informations DHCP v6 reçus. Ce type de message est envoyé par un client pour demander des informations de configuration autres que l'attribution d'adresse IP.
Paquets de transfert de relais DHCPv6 reçus	Le nombre de messages de transfert de relais DHCPv6 reçus. Ce type de message est envoyé par un agent relais pour transférer les messages aux serveurs.

Table 45 : Informations statistiques sur le serveur DHCPv6 (A continué)

Champ	Description
Paquets de réponse relais DHCPv6 reçus	Le nombre de messages de réponse de relais DHCP v6 reçus. Ce type de message est envoyé par un serveur à un agent relais DHCP v6 et contient le message que l'agent relais doit transmettre au client.
Paquets DHCPv6 mal formés reçus	Le nombre de messages DHCPv6 reçus mais abandonnés parce qu'ils étaient mal formés.
Paquets DHCPv6 reçus rejetés	Nombre de paquets rejetés.
Message envoyé	
Total des paquets DHCPv6 envoyés	Nombre de messages DHCPv6 envoyés. Les messages DHCPv6 envoyés d'un serveur DHCPv6 à un client DHCPv6 comprennent les messages Advertise, Reply, Reconfigure et Relay-Reply.
Paquets de publicité DHCPv6 transmis	Nombre de messages d'annonce DHCPv6 envoyés. Ce type de message est envoyé par un serveur à un client DHCPv6 en réponse à un message de sollicitation et indique que informatique est disponible pour le service.
Paquets de réponse DHCPv6 transmis	Nombre de messages de réponse DHCPv6 envoyés à un client DHCPv6 en réponse à un message de sollicitation, de demande, de renouvellement, de reliaison, de demande d'information, de confirmation, de publication ou de refus.
Paquets de reconfiguration DHCPv6 transmis	Nombre de messages de reconfiguration DHCPv6 envoyés. Ce type de message est envoyé par un serveur à un client DHCPv6 pour informer le client que le serveur dispose d'informations nouvelles ou mises à jour. Le client initie alors généralement une transaction de renouvellement/réponse ou de demande/réponse d'informations avec le serveur pour recevoir les informations mises à jour.
Paquets transmis par relais DHCPv6	Le nombre de messages DHCPv6 Relay-Forward envoyés. Ce type de message est envoyé par un agent relais pour transférer les messages aux serveurs.
Paquets de réponse relais DHCPv6 transmis	Le nombre de messages Relais-réponse DHCPv6 envoyés. Ce type de message est envoyé par un serveur à un agent relais DHCPv6 et contient le message que l'agent relais doit remettre au client.

Supprimez les statistiques DHCPv6 pour une ou toutes les interfaces

Pour supprimer les statistiques DHCPv6 pour une ou toutes les interfaces :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > services > serveur DHCPv6 > statistiques du serveur DHCPv6**.

La page statistiques du serveur DHCPv6 s'affiche.

6. Effectuez l'une des opérations suivantes :

- **Supprimer les statistiques d'une interface** : Dans le menu interface, sélectionnez l'interface.
- **Supprimer les statistiques pour toutes les interfaces** : Dans le menu interface, sélectionnez **tout**.

7. Cliquez sur le bouton **Clear** (Effacer).

Les statistiques sélectionnées sont supprimées.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Interface de relais DHCPv6

Un agent de relais DHCPv6 permet de joindre des sous-options aux messages qui sont relayés par le commutateur à un serveur DHCPv6. À son tour, le serveur DHCPv6 peut utiliser ces informations pour déterminer une adresse à attribuer à un client DHCPv6.

Pour configurer une interface en tant que relais DHCPv6 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > services > Relais DHCPv6** .

La page Configuration de l'interface DHCPv6 s'affiche.

6. Si une pile est configurée, indiquez si vous souhaitez afficher les interfaces physiques d'un commutateur ou de tous les commutateurs de la pile :

- **ID d'unité pour un commutateur empilé** : Les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.

Si aucune pile de commutateurs n'est configurée, la seule option est l'ID d'unité 1.

- **Tous:** Les interfaces physiques de tous les commutateurs de la pile sont affichées. Si aucune pile de commutateurs n'est configurée, l'option tous n'a aucun effet.

7. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :

- Pour afficher ou effacer les statistiques d'une seule interface, cochez la case associée à l'interface ou saisissez le numéro de l'interface dans le champ **aller à l'interface** et cliquez sur le bouton **aller**.
- Pour configurer plusieurs interfaces avec les mêmes paramètres, cochez la case associée à chaque interface.
- Pour configurer toutes les interfaces avec les mêmes paramètres, cochez la case dans la ligne d'en-tête.

8. Dans le menu **mode Admin**, sélectionnez pour activer ou désactiver le mode relais DHCPv6 sur l'interface.

❗ Remarque: Les fonctions de relais DHCPv6 et de serveur DHCPv6 sont mutuellement exclusives. Pour plus d'informations sur la configuration d'une interface en tant que serveur DHCPv6, reportez-vous à la section [Configurez les paramètres cos d'une interface](#) à la page 219.

9. Dans le menu **interface relais**, sélectionnez l'interface, lag ou VLAN connecté au serveur relais DHCPv6.

10. Dans le champ **adresse IP de destination**, spécifiez l'adresse IPv6 du serveur relais DHCPv6.

11. Dans le champ **ID distant**, spécifiez l'option informations sur l'agent relais.

L'ID distant est dérivé du DUID du serveur DHCPv6 et du numéro de l'interface de relais, ou vous pouvez spécifier est sous forme de chaîne définie par l'utilisateur.

12. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

13. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Power over Ethernet

Vous pouvez configurer les paramètres de configuration PoE (Power over Ethernet) globaux et les paramètres PoE pour chaque port.

Concepts PoE

Les modèles PoE (Power over Ethernet) prennent en charge les ports PoE+ ou PoE++ avec les capacités et les budgets de ports décrits dans les tableaux suivants.

Table 46 : Capacités des ports PoE

Modèle	Ports PoE	Capacité du port
M4350-24X4V	24 PoE+ (802.3at)	30 W
M4350-24G4XF	24 PoE+ (802.3at)	30 W
M4350-48G4XF	48 PoE+ (802.3at)	30 W
M4350-44M4X4V	48 PoE+ (802.3bt)	90 W
M4350-36X4V	36 PoE+ (802.3bt)	90 W
M4350-24X8F8V	24 PoE+ (802.3bt)	90 W
M4350-40X4C	40 PoE+ (802.3bt)	90 W

Table 47 : Budgets pour les switchs PoE

Modèle	Budget PoE du switch	
M4350-24X4V (1 baie d'alimentation pour points d'accès en option)	Bloc d'alimentation interne uniquement	576 W
	Ajoutez 1 APS350W	700 W
	Ajoutez 1 APS600Wv2 ¹	720 W
M4350-24G4XF (1 baie d'alimentation pour points d'accès en option)	Bloc d'alimentation interne uniquement	648 W
	Ajoutez 1 APS350W ²	720 W

Table 47 : Budgets pour les switchs PoE (A continué)

Modèle	Budget PoE du switch	
M4350-48G4XF (2 baies d'alimentation pour points d'accès en option)	Bloc d'alimentation interne uniquement	236 W
	Ajoutez 1 APS350W	436 W
	Ajoutez 1 APS600Wv2	636 W
	Ajoutez 1 APS920W	892 W
	Ajoutez 1 APS2000W à 110 V.	956 W
	Ajoutez 1 APS2000W à 220 V.	1440 W
	Ajoutez 2 APS350W	716 W
	Ajoutez 2 APS600Wv2	1116 W
	Ajoutez 2 APS920W	1440 W
	Ajoutez 2 APS2000W à 110 V.	1440 W
	Ajoutez 2 APS2000W à 220 V.	1440 W
M4350-44M4X4V (2 baies d'alimentation pour points d'accès en option)	Bloc d'alimentation interne uniquement	194 W
	Ajoutez 1 APS350W	394 W
	Ajoutez 1 APS600Wv2	594 W
	Ajoutez 1 APS920W	850 W
	Ajoutez 1 APS2000W à 110 V.	914 W
	Ajoutez 1 APS2000W à 220 V.	1786 W
	Ajoutez 2 APS350W	674 W
	Ajoutez 2 APS600Wv2	1074 W
	Ajoutez 2 APS920W	1586 W
	Ajoutez 2 APS2000W à 110 V.	1714 W
	Ajoutez 2 APS2000W à 220 V.	3314 W

Table 47 : Budgets pour les switchs PoE (A continué)

Modèle	Budget PoE du switch	
M4350-36X4V (1 baie d'alimentation pour points d'accès en option)	Bloc d'alimentation interne uniquement	280 W
	Ajoutez 1 APS600Wv3	640 W
	Ajoutez 1 APS1200Wv2 à 110 V.	960 W
	Ajoutez 1 APS1200Wv2 à 220 V.	1120 W
	Ajoutez 1 APS2000Wv2 à 110 V.	960 W
	Ajoutez 1 APS2000Wv2 à 220 V.	1760 W
M4350-24X8F8V (1 baie d'alimentation pour points d'accès en option)	Bloc d'alimentation interne uniquement	290 W
	Ajoutez 1 APS600Wv3	650 W
	Ajoutez 1 APS1200Wv2 à 110 V.	970 W
	Ajoutez 1 APS1200Wv2 à 220 V.	1130 W
	Ajoutez 1 APS2000Wv2 à 110 V.	970 W
	Ajoutez 1 APS2000Wv2 à 220 V.	1770 W
M4350-40X4C (1 baie d'alimentation pour points d'accès en option)	Bloc d'alimentation interne uniquement	196 W
	Ajoutez 1 APS600Wv3	556 W
	Ajoutez 1 APS1200Wv2 à 110 V.	876 W
	Ajoutez 1 APS1200Wv2 à 220 V.	1036 W
	Ajoutez 1 APS2000Wv2 à 110 V.	876 W
	Ajoutez 1 APS2000Wv2 à 220 V.	1676 W

1. Si vous installez un point d'accès plus puissant tel qu'un APS920W ou APS2000W, le budget PoE n'augmente pas.
2. Si vous installez un point d'accès plus puissant tel qu'un APS600Wv2, APS920W ou APS2000W, le budget PoE n'augmente pas.

L'alimentation fournie est traitée par priorité dans l'ordre croissant des ports, dans la limite du budget d'alimentation total de l'appareil. Le port PoE portant le numéro le plus bas (par exemple, le port 1) reçoit la priorité PoE la plus élevée, tandis que le port PoE portant le numéro le plus élevé (par exemple, le port 24) est relégué à la priorité PoE la plus basse.

Si les besoins en alimentation des appareils connectés dépassent le budget d'alimentation total du switch, l'appareil connecté au port PoE avec le numéro le plus

élevé ne sera plus alimenté pour que les appareils connectés aux ports PoE prioritaires (avec les numéros les moins élevés) soient d'abord pris en charge.

Bien qu'un périphérique puisse être répertorié comme un périphérique alimenté par PoE++ 802.3bt ou alimenté par PoE+ 802.3at, informatique peut ne pas exiger la limite de puissance maximale spécifiée par sa norme IEEE. De nombreux appareils nécessitent une puissance moindre, permettant ainsi aux quatre ports PoE de fonctionner simultanément lorsque les appareils reportent correctement leur classe PoE au switch.

Le tableau suivant montre les plages de puissance standard calculées avec une longueur de câble maximale de 100 mètres. Si un appareil reçoit une alimentation PoE insuffisante du switch, pensez à utiliser un câble plus court.

Table 48 : Classes PoE et allocations de puissance PoE

Classe d'appareil	Norme PoE compatible	Description de la classe	Puissance maximale réservée pour le PD	Puissance fournie à l'appareil alimenté
0	PoE, PoE+ et PoE++	Alimentation par défaut (complet)	15,4 W	0,44 W - 15,8 W
1	PoE, PoE+ et PoE++	Très basse consommation	4,0 W	0,44 W - 3,84 W
2	PoE, PoE+ et PoE++	Basse consommation	7,0 W	3,84 W - 7,2 W
3	PoE, PoE+ et PoE++	Consommation moyenne	15,4 W	6,49 W - 15,9 W
4	PoE+ et PoE++	Consommation élevée	30,0 W	12,95 W - 30,8 W
5	PoE++	Ultra-haute puissance	45,0 W	25,5 W - 47,0 W
6	PoE++	Ultra-haute puissance	90,0 W	51,0 W - 64,4 W
7	PoE++	Ultra-haute puissance	75,0 W	62,0 W - 81,1 W
8	PoE++	Ultra-haute puissance	90,0 W	71,0 W - 96,5 W

Définissez le seuil d'utilisation du système PoE et le mode de gestion de l'alimentation

Vous pouvez configurer un seuil pour le niveau d'utilisation PoE auquel une interruption est envoyée et vous pouvez définir le mode de gestion de l'alimentation que le commutateur utilise pour alimenter les périphériques alimentés (PD) demandeurs.

Pour définir le seuil d'utilisation du système PoE et le mode de gestion de l'alimentation :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez système > PoE > basique > Configuration PoE.

La page de configuration PoE s'affiche.

6. Si une pile est configurée, indiquez si vous souhaitez afficher les interfaces physiques d'un commutateur ou de tous les commutateurs de la pile :

- **ID d'unité pour un commutateur empilé** : Les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.

Si aucune pile de commutateurs n'est configurée, la seule option est l'ID d'unité 1.

- **Tous** : Les interfaces physiques de tous les commutateurs de la pile sont affichées. Si aucune pile de commutateurs n'est configurée, l'option tous n'a aucun effet.

7. Dans le champ **seuil d'utilisation du système**, entrez un nombre compris entre 1 et 99 pour définir le niveau de seuil auquel une interruption est envoyée si la puissance consommée dépasse le seuil de puissance.

8. Dans le menu **mode gestion de l'alimentation**, sélectionnez l'algorithme de gestion de l'alimentation que le commutateur utilise pour alimenter les DP demandeurs :

- Statique Sélectionnez **statique** pour spécifier que l'alimentation allouée à chaque port dépend du type de seuil d'alimentation configuré sur le port.
 - Dynamique Sélectionnez **dynamique** pour spécifier que la consommation d'énergie sur chaque port est mesurée et calculée en temps réel. Il s'agit de l'option par défaut.
9. Pour définir les interruptions, dans la section Configuration des interruptions PoE, sélectionnez l'un des boutons radio suivants :
- Activer. Active les interruptions PoE, ce qui signifie que le commutateur peut envoyer des interruptions PoE. Il s'agit de l'option par défaut.
 - Désactiver : Désactive les interruptions PoE, ce qui signifie que le commutateur ne peut pas envoyer d'interruptions PoE.
10. Cliquez sur le bouton **Apply** (Appliquer).
- Les paramètres sont enregistrés.
11. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 49 : Informations PoE

Champ	Description
Unité	L'unité est toujours 1, sauf si vous avez configuré une pile de commutateurs, auquel cas l'unité dépend du commutateur empilé.
Logement	L'emplacement est toujours 0.
Modèle	Le contrôleur PSE (Power Sourcing Equipment)
Hôte	Modèle de commutateur dans lequel le contrôleur PSE est installé
Version du micrologiciel (firmware)	Version du micrologiciel du contrôleur PSE
État de l'alimentation	État de l'alimentation (arrêt ou marche)
Puissance totale disponible (W)	Puissance maximale en watts que le commutateur peut fournir à tous les ports.
Seuil de puissance (W)	Si la puissance consommée est inférieure à la puissance seuil, le commutateur peut alimenter un autre port. La puissance consommée peut être comprise entre la puissance nominale et la puissance seuil. Le seuil de puissance est affiché en watts. Remarque : La valeur seuil de puissance est déterminée par la valeur que vous entrez dans le champ seuil d'utilisation du système.
Puissance consommée (W)	Puissance totale en watts fournie à tous les ports.

Configurez les paramètres du port PoE

Pour configurer les paramètres du port PoE :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez système > PoE > Avancé > Configuration du port PoE.

La page Configuration du port PoE s'affiche.

6. Si une pile est configurée, indiquez si vous souhaitez afficher les interfaces physiques d'un commutateur ou de tous les commutateurs de la pile :

- **ID d'unité pour un commutateur empilé** : Les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
Si aucune pile de commutateurs n'est configurée, la seule option est l'ID d'unité 1.
- **Tous** : Les interfaces physiques de tous les commutateurs de la pile sont affichées.
Si aucune pile de commutateurs n'est configurée, l'option tous n'a aucun effet.

7. Sélectionnez un ou plusieurs ports en effectuant l'une des actions suivantes :

- **Pour configurer un port unique, cochez la case associée au port ou tapez le numéro de port (par exemple g1) dans le champ aller à l'interface et cliquez sur le bouton aller.**
 - Pour configurer plusieurs ports avec les mêmes paramètres, cochez la case associée à chaque interface.
 - Pour configurer tous les ports avec les mêmes paramètres, cochez la case dans la ligne d'en-tête.
8. Dans le menu mode Admin, sélectionnez le mode PoE administratif du port :
- Activer. La capacité du port à fournir de l'énergie est désactivée. Il s'agit de l'option par défaut.
 - Désactiver : La capacité du port à fournir de l'énergie est désactivée.
9. Dans le menu Port Priority, sélectionnez la priorité du port par rapport aux autres ports si la puissance totale que le commutateur est capable de fournir dépasse le budget de puissance total :
- Faible : Priorité faible. Il s'agit de l'option par défaut.
 - Moyen(ne) Priorité moyenne
 - Elevé(e) : Priorité élevée
 - **Critique.** Priorité critique
- La priorité des ports détermine quels ports peuvent encore fournir de l'énergie lorsque la puissance totale fournie par le commutateur dépasse le budget d'alimentation total. (Dans une telle situation, le commutateur pourrait ne pas être en mesure de fournir de l'alimentation à tous les périphériques connectés.) Si la même priorité s'applique à deux ports, le port portant le numéro inférieur reçoit une priorité plus élevée.
10. Dans le menu mode puissance élevée, sélectionnez le mode PoE dans lequel le port doit fonctionner :
- 802.3af : Le port est alimenté et limité au mode IEEE 802.3af. Un périphérique alimentable en PoE qui requiert IEEE 802.3at ou IEEE 802.3bt ne reçoit pas d'alimentation si le port fonctionne en mode IEEE 802.3af.
 - Legacy HéritageLe port est alimenté par un courant d'appel élevé, ce qui est nécessaire pour les périphériques alimentables en PoE d'ancienne génération qui ont besoin de plus de 15 W pour se mettre sous tension.
 - Pre-802.3at Pré-802.3at Le port est initialement alimenté en mode IEEE 802.3af et, avant le passage de 75 ms, passe en mode IEEE 802.3at haute puissance. Sélectionnez ce mode si le périphérique alimentable en PoE n'exécute pas la classification de couche 2 ou si le commutateur exécute la classification decouche 1 de 2 événements.

- **802.3at** : Le port est alimenté en mode IEEE 802.3at et est rétrocompatible avec IEEE 802.3af. Le mode 802.3at est le mode par défaut. Dans ce mode, si le commutateur détecte que le périphérique alimentable en PoE connecté demande plus d'alimentation que la norme IEEE 802.3af mais qu'il ne s'agit pas d'un périphérique IEEE 802.3at de classe 4, ce périphérique ne reçoit pas d'alimentation du commutateur.
- **Pré-802.3bt** (modèles PoE++ uniquement) : Le port prend en charge les périphériques de classe 4 qui utilisent 4 paires PoE (4PPoE) pour recevoir une puissance supérieure à 30 W, mais qui ne sont pas conformes à la norme IEEE 802.3bt. Le port prend également en charge les modes IEEE 802.3at et IEEE 802.3af.
- **Type 802.3bt 3** (modèles PoE++ uniquement) : Le port prend en charge le mode IEEE 802.3bt type 3, le mode IEEE 802.3at et le mode IEEE 802.3af.
- **802 bt** (modèles PoE++ uniquement) : Le port est alimenté en mode IEEE 802.3bt et est rétrocompatible avec IEEE 802.3at et IEEE 802.3af. Dans ce mode, si le commutateur détecte que le périphérique alimentable en PoE connecté demande plus d'alimentation que la norme IEEE 802.3at mais qu'il ne s'agit pas d'un périphérique IEEE 802.3bt de classe 4, ce périphérique ne reçoit pas d'alimentation du commutateur.

11. Dans le menu **type de limite de puissance**, sélectionnez la manière dont le port contrôle la puissance maximale que l'informatique peut fournir :

- **Aucun** : Pour les ports PoE+ (802.3at), le port consomme jusqu'à la puissance maximale de classe 0 en mode économie d'énergie. En mode haute puissance, les conditions suivantes s'appliquent :
 - Ports PoE+ (802.3at) Le port consomme jusqu'à la puissance maximale de classe 4.
 - **Ports PoE++ (802.3bt)** (modèles PoE++ uniquement) : Le port consomme jusqu'à la puissance maximale de classe 8.
- **Classe** La limite de puissance du port est égale à la classe du PD connecté. Il s'agit de l'option par défaut. La limite supérieure est la puissance qu'un port peut fournir à un PD. La classe est détectée en fonction du PD qui est attaché au port, et les conditions suivantes s'appliquent :
 - Ports PoE+ (802.3at) Les valeurs possibles vont de la classe 0 à la classe 4.
 - **Ports PoE++ (802.3bt)** (modèles PoE++ uniquement) : Les valeurs possibles vont de la classe 0 à la classe 8.
- **Utilisateur** La limite de puissance du port est égale à la valeur spécifiée dans le champ **limite de puissance (W)**.

❗ **Remarque:** Si un PD ne signale pas correctement sa classe, l'utilisation de ces options peut préserver une puissance PoE supplémentaire en empêchant le commutateur de fournir plus de puissance que le PD n'en a besoin. Cependant, selon l'option sélectionnée, un PD qui ne signale pas correctement sa classe risque de ne pas se mettre sous tension du tout.

12. Dans le champ **limite de puissance (W)**, entrez la puissance maximale (en W) que le port peut fournir.

Ce qui suit s'applique :

- Ports PoE+ (802.3at) La gamme est de 3.0W à 30.0W.
- **Ports 802.3bt-Type3** (sélection dans le menu **mode d'alimentation** pour les modèles PoE++ uniquement) : La gamme est de 3.0W à 60.0W.
- **Ports PoE++ (802.3bt)** (modèles PoE++ uniquement) : La gamme est de 3.0W à 99.9W.

13. Dans le menu type de détection, sélectionnez la manière dont le port détecte le PD connecté :

- IEEE 802 Le port effectue une détection résistive à 4 points. Il s'agit de l'option par défaut.
- 4pt 802.3af + Legacy Le port effectue une détection résistive à 4 points et, si nécessaire, continue avec la détection héritée.
- Legacy Le port effectue une détection héritée.

14. Dans le menu calendrier, sélectionnez un calendrier ou sélectionnez aucun, qui est la sélection par défaut.

Pour plus d'informations sur la configuration des planifications de minuterie PoE, reportez-vous à la section Programmations de minuterie à la page 247.

15. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

16. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 50 : Informations sur le port PoE

Champ	Description
Consommation élevée	Tous les ports prennent en charge le mode haute puissance.
Puissance max. (W)	Puissance maximale en milliwatts pouvant être fournie par le port.

Table 50 : Informations sur le port PoE (A continué)

Champ	Description
Classe	La classe définit la plage de puissance qu'un périphérique alimenté (PD) tire du commutateur. Les définitions de classe sont les suivantes : • 0. 0,44 W - 15,8 W • 1. 0,44 W - 3,84 W • 2. 3,84 W - 7,2 W • 3. 6,49 W - 15,9 W • 4. 12,95 W - 30,8 W • 5. 25 W-47 W (modèles PoE++ uniquement) • 6. 51 W-64 W (modèles PoE++ uniquement) • 7. 62 W-81 W (modèles PoE++ uniquement) • 8. 71 W-96 W (modèles PoE++ uniquement) • Inconnu : La classe ne peut pas être détectée ou aucun PD n'est associé au port.
Tension de sortie (Volts)	Tension fournie au PD en volts.
Courant de sortie (mA)	Courant fourni au PD en mA.
Puissance de sortie (W)	Puissance fournie au PD en watts.
Etat	Status L'état opérationnel du port. • Désactivé : Aucune alimentation n'est fournie. • Distribution de la puissance La puissance est consommée par le PD. • Demande de puissance Le port demande de l'alimentation. • Echec Un problème est survenu au niveau de l'alimentation. • Test. Le port est en mode test. • Autre défaut : Le port est inactif en raison d'une condition d'erreur. • Recherche... Le port n'est pas dans l'un des autres états de cette liste.
Etat de la panne	Etat d'erreur Description de l'erreur lorsque le port PoE est en état d'erreur. • Aucune erreur: Le port n'est dans aucun état d'erreur et peut fournir de l'alimentation. • MPS absent Le port a détecté l'absence de l'alimentation principale, empêchant le port de fournir de l'énergie. • Court-circuit : Le port a détecté un court-circuit empêchant le port de fournir de l'alimentation. • Surcharge Le PD connecté au port tente de consommer plus d'énergie que ne le permettent les paramètres du port, empêchant le port de fournir de l'énergie. • Alimentation refusée Le port s'est vu refuser l'électricité en raison d'une pénurie d'électricité ou d'une condition administrative. Dans cet état,

Redémarrez un ou plusieurs ports PoE

Vous pouvez réinitialiser un ou plusieurs ports PoE. Cela peut être utile si les ports PoE ne fonctionnent pas comme prévu.

Pour réinitialiser un ou plusieurs ports PoE :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez système > PoE > Avancé > Configuration du port PoE.

La page Configuration du port PoE s'affiche.

6. Sélectionnez un ou plusieurs ports en effectuant l'une des actions suivantes :

- **Pour configurer un port unique, cochez la case associée au port ou tapez le numéro de port (par exemple g1) dans le champ aller à l'interface et cliquez sur le bouton aller.**
 - Pour configurer plusieurs ports avec les mêmes paramètres, cochez la case associée à chaque interface.
 - Pour configurer tous les ports avec les mêmes paramètres, cochez la case dans la ligne d'en-tête.
7. Cliquez sur le bouton **Power-cycle Port(s) (cycle d'alimentation des ports)**.
Les ports sont mis hors tension et hors tension.

Gérer le seuil d'utilisation de PoE

Si votre modèle est équipé de baies d'alimentation (également appelées logements), vous pouvez installer un ou plusieurs blocs d'alimentation auxiliaires (APS) pour étendre l'alimentation PoE ou activer la redondance de l'alimentation N+1 (voir [Gérer la redondance de l'alimentation N+1](#) à la page 243). En fonction du nombre de baies d'alimentation, vous pouvez également étendre l'alimentation PoE et activer la redondance d'alimentation N+1.

Le seuil d'utilisation du PoE s'applique au commutateur, c'est-à-dire à l'alimentation interne et à tout APSS optionnel installé.

Pour gérer le seuil d'utilisation PoE pour le commutateur :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > PoE > Avancé > Configuration de l'alimentation**.

La page Configuration de l'alimentation s'affiche.

6. Si une pile est configurée, dans le menu **ID UNITÉ**, sélectionnez l'ID d'un commutateur empilé.

7. Dans le champ **seuil d'utilisation du système**, entrez un nombre compris entre 1 et 99 pour définir le niveau de seuil auquel une interruption est envoyée si la puissance consommée dépasse le seuil de puissance.

La valeur que vous pouvez définir dans ce champ est la même que celle que vous pouvez définir dans le champ seuil d'utilisation du système de la page Configuration PoE (voir [Définissez le seuil d'utilisation du système PoE et le mode de gestion de l'alimentation](#) à la page 232).

8. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la section gestion de sources d'alimentation multiples.

Table 51 : Informations sur l'état de l'alimentation

Champ	Description
Puissance totale disponible (W)	Puissance maximale en watts de toutes les alimentations auxiliaires installées que le commutateur peut fournir à tous les ports
Puissance seuil PoE (W)	Si la puissance consommée est inférieure à la puissance seuil, le commutateur peut alimenter un autre port. La puissance consommée peut être comprise entre la puissance nominale et la puissance seuil. Le seuil de puissance est affiché en watts. Remarque : La valeur seuil de puissance est déterminée par la valeur que vous entrez dans le champ seuil d'utilisation du système.
Emplacement des modules d'alimentation	Baie PSU
Nom du module	Le numéro de modèle APS
Etat	L'état de l'APS : • Absent : Aucun point d'accès n'est installé ou détecté • Fonctionnement : L'APS est connecté et fonctionne correctement • Echec : Le contacteur ne peut pas détecter l'état • Non alimenté : L'APS est connecté mais pas sous tension.
Entrée CA du module d'alimentation (V)	La tension d'entrée CA de l'APS

Gérer la redondance de l'alimentation N+1

Si votre modèle est équipé de baies d'alimentation (PSU) (également appelées logements), vous pouvez installer une ou plusieurs alimentations auxiliaires (APSS) pour activer la redondance de l'alimentation N+1 ou étendre l'alimentation PoE (voir [Gérer le seuil d'utilisation de PoE](#) à la page 241). Selon le nombre de baies d'alimentation, vous pouvez également effectuer les deux.

Lorsque vous activez la redondance d'alimentation N+1, la puissance utilisable totale fournie par tous les APSS est égale à la puissance de tous les APSS moins la puissance d'un APS. La charge de puissance est répartie uniformément entre tous les APSS, qui se comportent comme s'ils étaient un seul point d'accès sans interruption de grande taille. Si un point d'accès tombe en panne, les deux autres points d'accès continuent à fournir de l'alimentation, permettant à tous les périphériques alimentés connectés de rester sous tension.

Pour gérer la redondance de l'alimentation N+1 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > PoE > Avancé > Configuration de l'alimentation**.

La page Configuration de l'alimentation s'affiche.

6. Pour activer ou désactiver la redondance de l'alimentation N+1, sélectionnez l'un des boutons radio suivants :

- Activer. Active la redondance de l'alimentation N+1. Les PD peuvent être mis hors tension si la puissance consommée dépasse la puissance disponible.
- Désactiver : Désactive la redondance de l'alimentation N+1. Il s'agit de l'option par défaut.

7. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la section gestion de sources d'alimentation multiples.

Table 52 : Informations PoE

Champ	Description
N+1 actif	Indique si N+1 est activé (Oui ou non)
Nombre d'unités d'alimentation	Nombre d'APSS connectés et actifs
Nombre effectif d'unités d'alimentation	Nombre d'APSS connectés et actifs lorsque le mode N+1 est activé

Affiche des informations sur la gestion de plusieurs sources d'alimentation pour l'alimentation PoE

L'alimentation PoE par défaut qu'un commutateur peut fournir dépend de l'alimentation interne. La puissance PoE *maximale* qu'un seul commutateur peut fournir dépend du nombre et des types d'alimentations auxiliaires optionnelles installées dans le commutateur.

Par exemple, le modèle M4350-48G4XF est livré avec une unité d'alimentation interne (PSU) et fournit deux baies d'alimentation pouvant accueillir différents types d'APSS (350 W, 600 W, 920 W ou 2000 W).

Le tableau de gestion des sources d'alimentation multiples (MPSM) affiche l'alimentation disponible pour les opérations PoE pour sept combinaisons possibles de ces trois alimentations (une alimentation interne et deux APS).

Pour afficher des informations sur la gestion de plusieurs sources d'alimentation :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > PoE > Avancé > Configuration de l'alimentation**.

La page Configuration de l'alimentation s'affiche.

Le tableau suivant décrit les champs en lecture seule de la section gestion de sources d'alimentation multiples.

Table 53 : Informations sur la gestion de plusieurs sources d'alimentation

Champ	Description
Rangée supérieure	
Unité	L'unité est toujours 1.
Logement	L'emplacement est toujours 0.
MPSM	L'index MPSM, qui dépend du nombre d'APSS installés dans le commutateur : • 0 : Condition anormale • 1 : Bloc d'alimentation interne uniquement • 2 : Points d'accès installés dans la baie d'alimentation 1 • 3 : Unité d'alimentation interne et points d'accès installés dans la baie d'alimentation 1 • 4 : Points d'accès installés dans la baie d'alimentation 2 • 5 : Unité d'alimentation interne et points d'accès installés dans la baie d'alimentation 2 • 6 : Points d'accès installés dans la baie d'unité d'alimentation 1 et points d'accès installés dans la baie d'unité d'alimentation 2 • 7 : Bloc d'alimentation interne, points d'accès installés dans la baie d'alimentation 1 et points d'accès installés dans la baie d'alimentation 2
Valeur de puissance MPSM	Puissance totale disponible en watts en fonction de l'unité d'alimentation interne et de l'APSS installé
Rangée inférieure	

Table 53 : Informations sur la gestion de plusieurs sources d'alimentation (A continué)

Champ	Description
Unité	L'unité est toujours 1.
Logement	L'emplacement est toujours 0.
MPSM-0 (W)	Puissance disponible en watts (W), bien que la condition ne soit pas normale
MPSM-1 (W)	Puissance disponible en W à partir de l'unité d'alimentation interne
MPSM-2 (W)	Alimentation disponible en W à partir de l'APS installé dans la baie d'alimentation 1
MPSM-3 (W)	Alimentation disponible en W provenant de l'unité d'alimentation interne et des points d'accès installés dans la baie d'alimentation 1
MPSM-4 (W)	Alimentation disponible en W à partir de l'APS installé dans la baie d'alimentation 2
MPSM-5 (W)	Alimentation disponible en W provenant de l'unité d'alimentation interne et des points d'accès installés dans la baie d'alimentation 2
MPSM-6 (W)	Alimentation disponible en W provenant des points d'accès installés dans la baie d'unité d'alimentation 1 et des points d'accès installés dans la baie d'unité d'alimentation 2
MPSM-7 (W)	Alimentation disponible en W provenant de l'unité d'alimentation interne, des points d'accès installés dans la baie d'alimentation 1 et des points d'accès installés dans la baie d'alimentation 2

Programmations de minuterie

Vous pouvez définir plusieurs programmations de minuterie (chacune portant un nom unique) que vous pouvez utiliser pour la fourniture d'alimentation PoE aux PD connectés et pour les listes de contrôle d'accès :

- **Programmations de temporisateurs à utiliser avec PoE :**

Après avoir créé une planification de minuterie, vous pouvez associer informatique à un ou plusieurs ports PoE (voir [Configurez les paramètres du port PoE](#) à la page 235). Vous pouvez également utiliser une planification de temporisation distincte pour chaque port PoE.

Une fois que vous avez associé une planification de minuterie à un port PoE, la date et l'heure de début forcent le port PoE à cesser de fournir de l'alimentation et la date et l'heure d'arrêt permettent au port PoE de *commencer* à fournir de l'alimentation.

- **Programmations de minuterie à utiliser avec les listes de contrôle d'accès :**

Après avoir créé une planification de minuterie, vous pouvez associer informatique à une ou plusieurs listes de contrôle d'accès (voir [Liste de contrôle d'accès](#) à la page 1028). Vous pouvez également utiliser une planification de minuterie distincte pour chaque liste de contrôle d'accès.

Vous pouvez créer des plannings de minuterie absolus, qui s'appliquent à des dates et heures spécifiques, et vous pouvez créer des plannings de minuterie récurrents. Pour chaque programme de minuterie, vous pouvez ajouter plusieurs entrées qui s'appliquent uniquement au programme de minuterie sélectionné.

Créez un programme de minuterie

Le nombre maximum de programmations de minuterie que vous pouvez ajouter est de 100.

Pour créer un planning de minuterie :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > planification minuterie > basique > Configuration globale**.

La page nom du calendrier s'affiche.

6. Dans le champ **nom du calendrier**, spécifiez le nom d'un calendrier.

7. Cliquez sur le bouton **Add** (Ajouter).

La planification de la minuterie est ajoutée au tableau de la page nom de la planification de la minuterie et un ID lui est attribué.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Spécifiez les paramètres d'une planification de minuterie PoE absolue .

Un calendrier de minuterie absolu s'applique à des dates et heures spécifiques. La planification est exécutée une seule fois.

Pour spécifier les paramètres d'une planification de minuterie qui utilise des dates et des heures spécifiques :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **système > programmation de la minuterie > Avancé > Configuration de la programmation de la minuterie** .
La page Configuration de la programmation du minuteur s'affiche.
6. Dans la section sélection du programme de minuterie, effectuez vos sélections dans les menus suivants :
 - a. **Nom de la programmation de la minuterie** . Sélectionnez le nom de la planification de minuterie que vous souhaitez configurer.
Vous ne pouvez sélectionner que les noms des horaires que vous avez créés (voir [Créez un programme de minuterie](#) à la page 248).
 - b. **Type de programme de minuterie** . Sélectionnez **absolu**.
Les champs de la section Configuration de la planification du minuteur peuvent s'ajuster pour vous permettre de configurer une planification du minuteur pour des dates et des heures spécifiques.
 - c. **Entrée de la programmation de la minuterie** . Pour ajouter une nouvelle entrée, sélectionnez **nouveau**.
La sélection d'une entrée existante vous permet d'apporter des modifications à cette entrée.
7. Dans la section Configuration de la programmation de la minuterie, spécifiez les heures et les dates :
 - a. Dans le champ **heure de début**, entrez l'heure au format HH :MM pour spécifier le moment où la planification de la minuterie doit commencer.
 - b. Dans le champ **fin de l'heure**, entrez l'heure au format HH :MM pour spécifier le moment où la planification du minuteur doit s'arrêter.
 - c. En regard du champ **date de début**, cliquez sur l'icône calendrier et utilisez les menus de la fenêtre contextuelle pour saisir la date au format JJ-LUN-AAAA afin de spécifier le moment où la planification du minuteur doit commencer.
 - d. En regard du champ **date de fin**, cliquez sur l'icône calendrier et utilisez les menus de la fenêtre contextuelle pour saisir la date au format JJ-LUN-AAAA afin de spécifier le moment où la planification du minuteur doit s'arrêter.
8. Cliquez sur le bouton **Add** (Ajouter).
L'entrée pour la planification de la minuterie est ajoutée.
9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Spécifiez les paramètres d'une planification de minuterie PoE récurrente .

Un planning récurrent vous permet de configurer un planning unique qui commence à une date particulière et qui se répète avec une date de fin spécifique ou indéfiniment.

Pour une planification de minuterie récurrente unique, vous pouvez ajouter une configuration de planification quotidienne, hebdomadaire et mensuelle. Cela signifie que ces méthodes de gestion ne s'excluent pas mutuellement, mais se complètent.

Pour spécifier les paramètres d'une planification de minuterie qui utilise un modèle récurrent :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > programmation de la minuterie > Avancé > Configuration de la programmation de la minuterie** .

La page Configuration de la programmation du minuteur s'affiche.

6. Dans la section sélection du programme de minuterie, effectuez vos sélections dans les menus suivants :

- a. **Nom du programme de minuterie** : Sélectionnez le nom de la planification de minuterie que vous souhaitez configurer.

Vous ne pouvez sélectionner que les noms des horaires que vous avez créés (voir Créez un programme de minuterie à la page 248).

- b. **Type de planning de minuterie** : Sélectionnez **périodique**.

Les champs de la section Configuration de la planification du minuteur peuvent s'ajuster pour vous permettre de configurer une planification du minuteur avec un modèle de récurrence.

- c. **Entrée de programmation de minuterie** : Pour ajouter une nouvelle entrée, sélectionnez **nouveau**.

La sélection d'une entrée existante vous permet d'apporter des modifications à cette entrée.

7. Dans la section Configuration de la planification du minuteur, spécifiez le modèle de récurrence :

- a. Dans le champ **heure de début**, entrez l'heure au format HH :MM pour spécifier le moment où la planification de la minuterie doit commencer.
- b. Dans le champ **fin de l'heure**, entrez l'heure au format HH :MM pour spécifier le moment où la planification du minuteur doit s'arrêter.
- c. En regard du champ **date de début**, cliquez sur l'icône calendrier et utilisez les menus de la fenêtre contextuelle pour saisir la date au format JJ-LUN-AAAA afin de spécifier le moment où la planification du minuteur doit commencer.
- d. Sélectionnez le bouton radio **aucune date de fin** ou sélectionnez le bouton radio **date de fin**, puis, à côté du champ **date de fin**, cliquez sur l'icône calendrier et utilisez les menus de la fenêtre contextuelle pour saisir la date au format JJ-LUN-AAAA afin de spécifier le moment où la planification du minuteur doit s'arrêter.
- e. Dans le menu **modèle de récurrence**, sélectionnez le modèle :

- **Tous les jours**. La planification de la minuterie fonctionne avec la récurrence quotidienne. Les champs s'ajustent.

Sélectionnez le bouton radio **tous les jours de la semaine** pour que le programme fonctionne du lundi au vendredi ou sélectionnez le bouton radio **tous les jours** et entrez un nombre compris entre 0 et 255 dans le champ.

Dans ce dernier cas, le planning est déclenché tous les jours spécifiés. Si le nombre de jours n'est pas spécifié, ou si vous saisissez 0, le planning n'est déclenché qu'une seule fois.

- **Hebdomadaire.** Le programme de minuterie fonctionne avec une périodicité hebdomadaire. Les champs s'ajustent.

Dans le champ **toutes les semaines**, entrez un nombre compris entre 0 et 255 pour spécifier que le planning doit être déclenché chaque nombre de semaines spécifié. Si le nombre de semaines n'est pas spécifié, ou si vous saisissez 0, le planning n'est déclenché qu'une seule fois.

Cochez une case un **jour de semaine**, plusieurs cases ou toutes les cases pour spécifier le ou les jours de la semaine que le programme doit exécuter.

- **Chaque mois** Le programme de minuterie fonctionne avec une récurrence mensuelle. Les champs s'ajustent.

Dans le champ **jour**, entrez un nombre compris entre 1 et 31 pour spécifier le jour du mois où le planning doit être déclenché.

Dans le champ **tous les mois**, entrez un nombre compris entre 0 et 99 pour spécifier que le planning doit être déclenché tous les mois spécifiés. Si le nombre de mois n'est pas spécifié, ou si vous saisissez 0, le planning n'est déclenché qu'une seule fois.

8. Cliquez sur le bouton **Add** (Ajouter).

L'entrée pour la planification de la minuterie est ajoutée.

9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Modifiez les paramètres d'une entrée de planification de minuterie PoE récurrente .

Vous pouvez modifier les paramètres d'une entrée de planification de minuterie récurrente existante. (Vous ne pouvez pas effectuer cette opération pour une planification de minuterie absolue existante.)

Pour modifier les paramètres d'une entrée de programmation récurrente existante :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > programmation de la minuterie > Avancé > Configuration de la programmation de la minuterie**.

La page Configuration de la programmation du minuteur s'affiche.

6. Dans le menu **nom de la programmation**, sélectionnez le nom de la programmation.

7. Dans le menu **type de planning**, sélectionnez le type de planning.

8. Dans le menu **entrée de programmation de la minuterie**, sélectionnez l'entrée de programmation.

9. Apportez les modifications à l'entrée de planification.

Pour plus d'informations, consultez [Spécifiez les paramètres d'une planification de minuterie PoE récurrente](#), à la page 251.

10. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

11. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimer une entrée de programmation de minuterie

Vous pouvez supprimer une entrée de programmation dont vous n'avez plus besoin.

Pour supprimer une entrée de programmation de minuterie :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > programmation de la minuterie > Avancé > Configuration de la programmation de la minuterie**.

La page Configuration de la programmation du minuteur s'affiche.

6. Dans le menu **nom de la programmation**, sélectionnez le nom de la programmation.
7. Dans le menu **type de planning**, sélectionnez le type de planning.
8. Dans le menu **entrée de programmation de la minuterie**, sélectionnez l'entrée de programmation.
9. Cliquez sur le bouton **Supprimer**.

L'entrée est supprimée.

10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimer un planning de minuterie

Vous pouvez supprimer un planning de minuterie dont vous n'avez plus besoin. Toutes les entrées qui font partie de la planification de la minuterie sont également supprimées.

Pour supprimer un programme de minuterie :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > planification minuterie > basique > Configuration globale**.

La page nom du calendrier s'affiche.

6. Cochez la case correspondant au planning à supprimer.

7. Cliquez sur le bouton **Supprimer**.

Le planning est supprimé.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Simple Network Management Protocol

Vous pouvez configurer les paramètres SNMP pour SNMPv1/SNMPv2 et SNMPv3. Le commutateur prend en charge la configuration des groupes SNMP et des utilisateurs qui peuvent gérer les interruptions générées par l'agent SNMP.

Le commutateur utilise à la fois des MIB publiques standard pour la fonctionnalité standard et des MIB privées qui prennent en charge des fonctionnalités de commutateur supplémentaires.

Gérer les communautés SNMPv1 et SNMPv2

Par défaut, aucune communauté SNMP n'existe. Les communautés que vous définissez peuvent accéder au commutateur à l'aide de SNMPv1 et SNMPv2. Seules les communautés disposant d'un accès de niveau lecture/écriture peuvent être utilisées pour modifier la configuration à l'aide de SNMP.

Ajoutez une communauté SNMPv1 et SNMPv2

Vous pouvez ajouter une communauté SNMPv1 et SNMPv2, qui autorise à la fois l'accès SNMPv1 et SNMPv2.

Pour ajouter une communauté SNMPv1 et SNMPv2 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez System > SNMP > SNMP V1/V2 > Community Configuration.

La page Configuration de la communauté s'affiche.

6. Dans le champ **nom de communauté**, entrez le nom d'une nouvelle communauté.
Le nom peut comporter jusqu'à 16 caractères.

7. Spécifiez l'adresse IP du client et le masque IP du client :

- **Adresse du client** : Saisissez l'adresse IPv4 ou IPv6 du client.
- **Longueur du masque IPv4/préfixe IPv6 du client** : Entrez le masque IPv4 d'un client IPv4 ou la longueur du préfixe IPv6 d'un client IPv6.

L'adresse IP du client et la longueur du masque ou du préfixe IP du client désignent une plage d'adresses IP à partir desquelles les clients SNMP peuvent utiliser la communauté pour accéder au commutateur.

Pour les clients IPv4, si l'adresse IP ou le masque IP du client est 0,0,0,0, l'accès est autorisé à partir de n'importe quelle adresse IP. Sinon, l'adresse IP de chaque client est ANDed avec le masque, tout comme l'adresse IP du client. Si les valeurs sont égales, l'accès est autorisé.

Par exemple, si l'adresse IPv4 du client et le masque IP du client sont 192.168.1,0/255.255.255.0, tout client IPv4 dont l'adresse IP est comprise entre 192.168.1.0 et 192.168.1.255 (inclus) est autorisé à accéder. Pour autoriser l'accès à partir d'une seule station IPv4, utilisez une valeur de masque IP de station de gestion de 255.255.255.255, et utilisez l'adresse IP de cet ordinateur comme adresse client.

8. Dans le menu **mode d'accès**, sélectionnez le niveau d'accès pour cette communauté, qui est **lecture-écriture** ou **lecture seule**.
9. Cliquez sur le bouton **Add** (Ajouter).

La communauté est ajoutée.

10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Modifier une communauté SNMPv1 et SNMPv2 existante

Vous pouvez modifier une communauté SNMPv1 et SNMPv2 existante.

Pour modifier une communauté SNMPv1 et SNMPv2 existante :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur principale à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez System > SNMP > SNMP V1/V2 > Community Configuration.

La page Configuration de la communauté s'affiche.

6. Cochez la case en regard de la communauté.

7. Modifiez les paramètres en fonction de vos besoins.

Pour plus d'informations sur les paramètres, reportez-vous à la section Ajoutez une communauté SNMPv1 et SNMPv2 à la page 257.

8. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimez une communauté SNMPv1 et SNMPv2

Vous pouvez supprimer une communauté SNMPv1 et SNMPv2 dont vous n'avez plus besoin.

Pour supprimer une communauté SNMPv1 et SNMPv2 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez System > SNMP > SNMP V1/V2 > Community Configuration.

La page Configuration de la communauté s'affiche.

6. Cochez la case en regard de la communauté.

7. Cliquez sur le bouton **Supprimer**.

La communauté est supprimée.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Gérez les paramètres de routage SNMPv1 et SNMPv2

Pour chaque communauté SNMP, vous pouvez spécifier l'interface source à utiliser sur le commutateur, le nom de communauté, l'adresse IP associée et d'autres paramètres.

Ajoutez une configuration d'interruption SNMPv1 ou SNMPv2 pour un hôte

Vous pouvez ajouter une configuration d'interruption pour un hôte, permettant à l'hôte de recevoir des interruptions SNMPv1 ou SNMPv2.

Pour ajouter une configuration d'interruption SNMPv1 ou SNMPv2 pour un hôte :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > SNMP > SNMP V1/V2 > Trap Configuration**.

La page Configuration des interruptions s'affiche.

6. Dans le menu **interface source**, sélectionnez l'interface source à utiliser pour le récepteur d'interruptions SNMP. Par défaut, les options suivantes s'affichent dans le menu :

- **Aucun** : L'adresse IP principale de l'interface d'origine (sortante) est utilisée comme adresse source.
- **VLAN 1** L'adresse IP principale de VLAN 1 est utilisée comme adresse source. Il s'agit de la sélection par défaut.
- **Port de service** L'adresse IP du port de gestion est utilisée comme adresse source.

Selon la configuration de votre commutateur, les options suivantes peuvent s'afficher :

- **Un autre identifiant VLAN** : L'adresse IP principale d'un VLAN autre que VLAN 1 est utilisée comme adresse source.
- **Interface de routage** : L'adresse IP principale d'une interface de routage est utilisée comme adresse source.
- **VLAN de routage** L'adresse IP principale d'une interface de routage VLAN est utilisée comme adresse source.
- **Interface de bouclage de routage** : L'adresse IP principale d'une interface de bouclage de routage est utilisée comme adresse source.
- **Différent**: Pour certaines fonctionnalités, *différents* peuvent s'afficher. Cela signifie que l'interface source est configurée séparément.

7. Dans le champ **nom de communauté**, spécifiez le nom de la communauté SNMP qui inclut l'hôte de gestion SNMP et l'agent SNMP sur le périphérique.

Le nom peut comporter jusqu'à 16 caractères et est sensible à la casse.

8. Dans le menu **version**, sélectionnez la version SNMP à utiliser par le récepteur :

- **SNMPv1** : Le commutateur utilise SNMPv1 pour envoyer des interruptions au récepteur. Le paramètre par défaut est SNMPv1.
- **SNMPv2** : Le commutateur utilise SNMPv2 pour envoyer des interruptions au récepteur.

9. Dans le menu **Protocole**, sélectionnez le protocole à utiliser par le récepteur :

Sélectionnez IPv4 si l'adresse du destinataire est IPv4 ou IPv6 si l'adresse du destinataire est IPv6. Vous pouvez également sélectionner **DNS** et saisir un nom de domaine.

10. Dans le champ **adresse**, entrez l'adresse IPv4 ou IPv6 ou le nom de domaine, selon votre sélection dans le menu **Protocole**.
11. Dans le menu **État**, sélectionnez pour activer ou désactiver le déROUTement :
 - Activer. La trappe est activée.
 - Désactiver : Le déROUTement est configuré mais désactivé.
12. Cliquez sur le bouton **Add** (Ajouter).

La configuration de trappe est ajoutée.
13. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Modifier une configuration d'interruption SNMPv1 ou SNMPv2 pour un hôte

Vous pouvez modifier une configuration d'interruption SNMPv1 ou SNMPv2 existante pour un hôte.

Pour modifier une configuration d'interruption SNMPv1 ou SNMPv2 pour un hôte :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.
4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > SNMP > SNMP V1/V2 > Trap Configuration**.

La page Configuration des interruptions s'affiche.

6. Cochez la case en regard de la configuration de trappe.

7. Modifiez les paramètres en fonction de vos besoins.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Ajoutez une configuration d'interruption SNMPv1 ou SNMPv2 pour un hôte](#) à la page 261.

8. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimez une configuration d'interruption SNMPv1 ou SNMPv2 pour un hôte

Vous pouvez supprimer une configuration d'interruption SNMPv1 ou SNMPv2 dont vous n'avez plus besoin pour un hôte.

Pour supprimer une configuration d'interruption SNMPv1 ou SNMPv2 pour un hôte :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **système > SNMP > SNMP V1/V2 > Trap Configuration**.
La page Configuration des interruptions s'affiche.
6. Cochez la case en regard de la configuration de trappe.
7. Cliquez sur le bouton **Supprimer**.
La configuration des interruptions est supprimée.
8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurer les drapeaux d'interruption SNMPv1 et SNMPv2 .

Vous pouvez activer ou désactiver des recouvrements spécifiques. Lorsque la condition identifiée par une interruption active se produit sur le commutateur, un message d'interruption est envoyé à tous les récepteurs d'interruption SNMP activés et un message est écrit dans le journal d'interruption.

Pour configurer les indicateurs de déroutement :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > SNMP > SNMP V1/V2 > Trap Flags**.

La page drapeaux de recouvrement s'affiche.

6. Pour un ou plusieurs indicateurs de déroutement affichés dans le tableau suivant, sélectionnez le bouton radio **désactiver** ou **Activer**.

Cette sélection active ou désactive l'activation de la trappe.

Piège	Par défaut	Comportement lorsqu'il est activé
Authentification	Activer	Une interruption est envoyée lorsqu'un événement impliquant une authentification se produit, par exemple lorsqu'un utilisateur tente d'accéder à l'interface utilisateur principale du commutateur et ne fournit pas de nom d'utilisateur et de mot de passe valides.
Liaison haut/bas	Activer	Une interruption est envoyée lorsque l'état administratif ou opérationnel d'une liaison physique ou logique change.
Utilisateurs multiples	Activer	Une interruption est envoyée lorsque le même ID utilisateur est connecté au commutateur plusieurs fois en même temps (via Telnet ou le port série).
Spanning Tree	Activer	Une interruption est envoyée lorsqu'un changement de Spanning Tree se produit.
Listes de contrôle d'accès (ACL)	Désactiver	Une interruption est envoyée lorsqu'une ACL est déclenchée.
Portail captif	Désactiver	Une interruption est envoyée lorsqu'un utilisateur accède à un portail captif.
DVMRP	Désactiver	Une interruption est envoyée lorsqu'une modification de la configuration DVMRP se produit.
PIM	Désactiver	Une interruption est envoyée lorsqu'une modification de la configuration PIM se produit.
PoE (Modèles PoE uniquement)	Désactiver	Une interruption est envoyée lorsqu'une modification de la configuration PoE se produit.

(A continué)

Piège	Par défaut	Comportement lorsqu'il est activé
Interruptions OSPFv2		
Erreurs		
Echec de l'authentification.	Désactiver	Une interruption est envoyée lorsqu'un échec d'authentification OSPFv2 se produit.
Paquets défaillants	Désactiver	Une interruption est envoyée lorsqu'un paquet OSPFv2 corrompu est détecté.
Erreur de configuration	Désactiver	Une interruption est envoyée lorsqu'une erreur de configuration OSPFv2 se produit.
Échec-authentification-virt	Désactiver	Une interruption est envoyée lorsqu'un échec d'authentification OSPFv2 virtuel se produit.
Virt-Bad-packet	Désactiver	Une interruption est envoyée lorsqu'un paquet OSPFv2 virtuel corrompu est détecté.
Erreur-config-virt	Désactiver	Une interruption est envoyée lorsqu'une erreur de configuration OSPFv2 virtuelle se produit.
LSA		
LSA-maxage	Désactiver	Une interruption est envoyée lorsque l'âge maximal d'une annonce d'état de lien (LSA) OSPFv2 est dépassé.
Origine LSA	Désactiver	Une interruption est envoyée lorsqu'un LSA OSPFv2 provient du commutateur (ou de l'une de ses interfaces de routage), par exemple, lorsque la topologie change.
Débordement		
Lsdb-overflow	Désactiver	Une interruption est envoyée lorsque la base de données d'état des liens (LSDB) OSPFv2 est en débordement, c'est-à-dire que la LSDB ne peut plus être maintenue en raison de contraintes de ressources.
Lsdb-approche-dépassement	Désactiver	Une interruption est envoyée lorsqu'un seuil critique de la taille de la carte LSDB OSPFv2 est dépassé.
Retransmettre		
Paquets	Désactiver	Une interruption est envoyée lorsqu'un paquet OSPFv2 est retransmis.
Virt-paquets	Désactiver	Une interruption est envoyée lorsqu'un paquet OSPFv2 virtuel est retransmis.
Changement d'état		

(A continué)

Piège	Par défaut	Comportement lorsqu'il est activé
Si-état-changement	Désactiver	Une interruption est envoyée lorsque l'état d'une interface OSPFv2 change.
Changement-état-voisin	Désactiver	Une interruption est envoyée lorsque l'état d'un voisin OSPFv2 change.
Virtif-State-change	Désactiver	Une interruption est envoyée lorsque l'état d'une interface OSPFv2 virtuelle change.
VirtNeighbor-State-change	Désactiver	Une interruption est envoyée lorsque l'état d'un voisin OSPFv2 virtuel change.
Interruptions OSPFv3		
Erreurs		
Paquets défaillants	Désactiver	Une interruption est envoyée lorsqu'un paquet OSPFv3 corrompu est détecté.
Erreur de configuration	Désactiver	Une interruption est envoyée lorsqu'une erreur de configuration OSPFv3 se produit.
Virt-Bad-packet	Désactiver	Une interruption est envoyée lorsqu'un paquet OSPFv3 virtuel corrompu est détecté.
Erreur-config-virt	Désactiver	Une interruption est envoyée lorsqu'une erreur de configuration OSPFv3 virtuelle se produit.
LSA		
LSA-maxage	Désactiver	Une interruption est envoyée lorsque l'âge maximal d'une annonce d'état de lien (LSA) OSPFv3 est dépassé.
Origine LSA	Désactiver	Une interruption est envoyée lorsqu'un LSA OSPFv3 provient du commutateur (ou de l'une de ses interfaces de routage), par exemple, lorsque la topologie change.
Débordement		
Lsdb-overflow	Désactiver	Une interruption est envoyée lorsque la base de données d'état des liens (LSDB) OSPFv3 est en débordement, c'est-à-dire que la LSDB ne peut plus être maintenue en raison de contraintes de ressources.
Lsdb-approche-dépassement	Désactiver	Une interruption est envoyée lorsqu'un seuil critique de la taille de la carte LSDB OSPFv3 est dépassé.
Retransmettre		
Paquets	Désactiver	Une interruption est envoyée lorsqu'un paquet OSPFv3 est retransmis.
Virt-paquets	Désactiver	Une interruption est envoyée lorsqu'un paquet OSPFv3 virtuel est retransmis.

(A continué)

Piège	Par défaut	Comportement lorsqu'il est activé
Changement d'état		
Si-état-changement	Désactiver	Une interruption est envoyée lorsque l'état d'une interface OSPFv3 change.
Changement-état-voisin	Désactiver	Une interruption est envoyée lorsque l'état d'un voisin OSPFv3 change.
Virtif-State-change	Désactiver	Une interruption est envoyée lorsque l'état d'une interface OSPFv3 virtuelle change.
VirtNeighbor-State-change	Désactiver	Une interruption est envoyée lorsque l'état d'un voisin OSPFv3 virtuel change.
État du module d'alimentation	Activer	Une interruption est envoyée lorsque l'état d'une alimentation auxiliaire (APS, également appelée unité d'alimentation externe [PSU]) change. Par exemple, une interruption est envoyée si un APS est inséré, supprimé, devient opérationnel ou perd de l'alimentation, ou si un avertissement est généré pour l'APS ou s'il échoue.
Etat FAN	Activer	Une interruption est envoyée lorsque l'état d'un module de ventilateur change. Par exemple, une interruption est envoyée si un module de ventilateur est interrompu ou retiré, ou si un avertissement est généré pour le module de ventilateur ou si le module de ventilateur tombe en panne.
Etat de la température	Activer	Un piège est envoyé lorsqu'un seuil critique de température est dépassé ou si la température s'écarte de sa plage normale.
VRRP	Activer	Une interruption est envoyée lorsque l'une des conditions suivantes est détectée : - ID de routeur vierge non valide - Erreurs TTL IP - Version non valide ou non prise en charge - Echec de la somme de contrôle - Type d'authentification invalide. - Incompatibilité du type d'authentification avec le paquet VRRP par rapport au type d'authentification configuré localement - Echec de l'authentification. - Nouvelle élection principale VRRP
Notification MAC	Désactiver	Une interruption est envoyée lorsque l'une des conditions suivantes est détectée : - Nouvelle entrée (adresse MAC) dans la base de données de transfert (FDB) - Suppression d'une entrée existante du FDB - Modification d'une entrée existante dans le FDB

7. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Afficher les MIB prises en charge

Pour afficher les MIB prises en charge par le commutateur :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.
Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur principale à la page 46.
4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **système > SNMP > SNMP V1/V2 > MIB prises en charge** .
La page MIB prises en charge s'affiche.
Le champ nom affiche le numéro RFC, le cas échéant, et le nom de la MIB.
Le champ Description affiche le titre RFC ou la description MIB.

Gérer les utilisateurs SNMPv3

Vous pouvez gérer les comptes utilisateur SNMPv3 et configurer l'authentification et le cryptage.

Ajoutez un compte utilisateur SNMPv3

Vous pouvez ajouter un compte utilisateur SMPv3.

Pour ajouter un compte utilisateur SNMPv3 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur principale à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez System > SNMP > SNMP V1/V3 > Community Configuration.

La page Configuration utilisateur s'affiche.

6. Dans le champ **nom d'utilisateur**, saisissez un nom pour le compte d'utilisateur.

Le nom peut comporter jusqu'à 30 caractères.

7. Dans le menu **SNMP v3 Access mode**, sélectionnez **Read-Only** ou **Read/Write** pour spécifier les privilèges d'accès SNMPv3 pour le compte d'utilisateur.

Les privilèges d'accès SNMPv3 pour le compte admin sont lecture/écriture.

8. Dans le menu **Protocole d'authentification**, sélectionnez **SHA512** pour l'authentification.

SHA512 est le seul choix possible dans le menu.

9. Dans le champ **Authentication Key** (clé **d'authentification**), saisissez un mot de passe (clé).

Le mot de passe peut comporter jusqu'à 32 caractères.

10. Dans le menu **Protocole de cryptage**, sélectionnez **aucun** ou **AES128** pour le cryptage :

- **Aucun** : Les informations ne sont pas cryptées.
- **AES128** : Vous devez spécifier un mot de passe de cryptage pour l'accès SNMPv3 (voir l'étape suivante).

11. Si vous sélectionnez **AES128** dans le menu **Encryption Protocol**, spécifiez un mot de passe (clé) dans le champ **Encryption Key**.

Le mot de passe peut comporter jusqu'à 32 caractères.

12. Cliquez sur le bouton **Add** (Ajouter).

Le compte utilisateur SNMPv3 est ajouté.

13. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Modifier un compte utilisateur SNMPv3

Vous pouvez modifier un compte utilisateur SMPv3 existant.

Pour modifier un compte utilisateur SNMPv3 existant :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez System > SNMP > SNMP V1/V3 > Community Configuration.

La page Configuration utilisateur s'affiche.

6. Cochez la case en regard du compte utilisateur SNMPv3.

7. Modifiez les paramètres en fonction de vos besoins.

Pour plus d'informations sur les paramètres, reportez-vous à la section .

8. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimer un compte utilisateur SNMPv3

Vous pouvez supprimer un compte utilisateur SMPv3 dont vous n'avez plus besoin.

Pour supprimer un compte utilisateur SNMPv3 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez System > SNMP > SNMP V1/V3 > Community Configuration.

La page Configuration utilisateur s'affiche.

6. Cochez la case en regard du compte utilisateur SNMPv3.

7. Cliquez sur le bouton **Supprimer**.

Le compte utilisateur SNMPv3 est supprimé.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

LLDP (Link Layer Discovery Protocol)

Le protocole LLDP (Link Layer Discovery Protocol), défini dans IEEE 802.1AB, permet aux périphériques d'un réseau local d'annoncer les principales fonctionnalités et descriptions physiques. Vous pouvez afficher ces informations pour identifier la topologie du système et détecter les configurations problématiques dans le LAN.

LLDP est un protocole unidirectionnel sans séquences de requête et de réponse. Les informations sont annoncées par les périphériques configurés pour transmettre LLDP et sont reçues et traitées par les périphériques configurés pour recevoir LLDP. Vous pouvez activer et désactiver les fonctions de transmission et de réception séparément par port. Par défaut, les fonctions de transmission et de réception sont désactivées sur tous les ports.

Configurez les paramètres LLDP globaux

Vous pouvez spécifier des paramètres LLDP qui sont appliqués globalement au commutateur.

Pour configurer les paramètres LLDP globaux :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > LLDP > Configuration globale**.

La page Configuration globale s'affiche.

6. Dans le champ **intervalle annoncé TLV**, entrez l'intervalle en secondes pour transmettre les trames LLDP.

La plage est de 5 à 32768 secondes. La valeur par défaut est de 30 secondes.

7. Dans le champ **multiplicateur d'attente**, entrez le multiplicateur de la valeur que vous entrez dans le champ **intervalle annoncé TLV**, qui détermine le temps de vie (TTL) pour les notifications LLDP.

La plage est de 2 à 10 secondes. La valeur par défaut est 4. Par exemple, si la valeur que vous entrez dans le champ **intervalle annoncé TLV** est 30 et que la valeur que

vous entrez dans le champ **multiplicateur d'attente** est 4, le TTL pour les notifications LLDP est de 120 secondes.

8. Dans le champ **délai de réinitialisation**, entrez le délai avant le début de la réinitialisation.

La plage est de 1 à 10 secondes. La valeur par défaut est de 2 secondes.

9. Dans le champ **intervalle de notification**, entrez l'intervalle en secondes pour la transmission des notifications.

La plage est de 5 à 3600 secondes. La valeur par défaut est de 5 secondes.

10. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

11. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurer les paramètres de l'interface LLDP

Vous pouvez spécifier des paramètres LLDP appliqués à une ou plusieurs interfaces.

Pour configurer les paramètres de l'interface LLDP :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **système > LLDP > Configuration de l'interface** .
La page Configuration de l'interface s'affiche.
6. Si une pile est configurée, indiquez si vous souhaitez afficher les interfaces physiques d'un commutateur ou de tous les commutateurs de la pile :
 - **ID d'unité pour un commutateur empilé** : Les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
Si aucune pile de commutateurs n'est configurée, la seule option est l'ID d'unité 1.
 - **Tous**: Les interfaces physiques de tous les commutateurs de la pile sont affichées.
Si aucune pile de commutateurs n'est configurée, l'option tous n'a aucun effet.
7. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :
 - Pour afficher ou effacer les statistiques d'une seule interface, cochez la case associée à l'interface ou saisissez le numéro de l'interface dans le champ **aller à l'interface** et cliquez sur le bouton **aller**.
 - Pour configurer plusieurs interfaces avec les mêmes paramètres, cochez la case associée à chaque interface.
 - Pour configurer toutes les interfaces avec les mêmes paramètres, cochez la case dans la ligne d'en-tête.

Les champs État du lien indiquent si l'interface est active ou inactive.
8. Dans le menu **transmettre**, sélectionnez si l'interface peut transmettre des notifications LLDP.
La valeur par défaut est Activer.
9. Dans le menu **recevoir**, sélectionnez si l'interface peut recevoir des notifications LLDP.
La valeur par défaut est Activer.
10. Dans le menu **notifier**, indiquez si l'interface peut prendre en charge les notifications LLDP.
La valeur par défaut est désactiver.
11. En option, configurez les informations suivantes sur la valeur de longueur de type (TLV), qui sont toutes activées par défaut :

- Description des ports Sélectionnez si l'interface peut envoyer une description de port dans une trame LLDP.
 - **Nom du système** : Sélectionnez si l'interface peut envoyer le nom du système dans une trame LLDP.
 - **Description du système** : Sélectionnez si l'interface peut envoyer la description du système dans une trame LLDP.
 - **Capacités du système** : Sélectionnez si l'interface peut envoyer les capacités du système dans une trame LLDP.
12. Dans le menu **informations de gestion**, sélectionnez si l'adresse de gestion est transmise dans des trames LLDP.
13. Cliquez sur le bouton **Apply** (Appliquer).
- Les paramètres sont enregistrés.
14. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Afficher ou effacer les statistiques LLDP

Pour afficher ou effacer les statistiques LLDP :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **système > LLDP > statistiques**.
La page statistiques s'affiche.
6. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).
7. Pour effacer toutes les statistiques LLDP, cliquez sur le bouton **Effacer**.
Toutes les statistiques sont effacées.
8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 54 : Informations statistiques LLDP

Champ	Description
Statistiques LLDP	
Ces statistiques concernent le commutateur.	
Dernière mise à jour	Heure à laquelle une entrée a été créée, modifiée ou supprimée dans les tables associées au système distant.
Nombre total d'inserts	Nombre de fois que l'ensemble complet d'informations annoncées par un point d'accès au service MAC (MSAP) particulier a été inséré dans des tables associées aux systèmes distants.
Nombre total de suppressions	Nombre de fois que l'ensemble complet des informations annoncées par un point d'accès au service MAC (MSAP) particulier a été supprimé des tables associées aux systèmes distants.
Nombre total de chutes	Nombre de fois que l'ensemble complet des informations annoncées par un point d'accès au service MAC (MSAP) particulier n'a pas pu être entré dans les tables associées aux systèmes distants en raison de ressources insuffisantes.
Ageouts totaux	Nombre de fois que l'ensemble complet d'informations annoncées par un point d'accès de service MAC (MSAP) particulier a été supprimé des tables associées aux systèmes distants parce que l'intervalle de temps d'information a expiré.
Statistiques LLDP	
Les statistiques Thérèse sont pour les interfaces.	
Interface	L'interface.
Total transmission	Nombre de trames LLDP transmises par l'agent LLDP.
Total de réception	Nombre de trames LLDP valides reçues par cet agent LLDP.

Table 54 : Informations statistiques LLDP (A continué)

Champ	Description
ABANDONNER	Nombre de TLV LLDP supprimés par l'agent LLDP pour quelque raison que ce soit.
Erreurs	Nombre de trames LLDP non valides reçues par l'agent LLDP.
Ageouts	Le nombre de dépassements de âge qui se sont produits. Une expiration est le nombre de fois où l'ensemble complet d'informations annoncées par un point d'accès de service MAC (MSAP) particulier a été supprimé des tables associées aux entrées distantes parce que l'intervalle de temps d'information a expiré.
TLV rejets	Nombre de TLV LLDP éliminés par l'agent LLDP.
TLV inconnues	Nombre de TLV LLDP reçus qui n'ont pas été reconnus par l'agent LLDP.
TLV MED	Nombre total de TLV LLDP-MED reçus.
TLV 802,1	Nombre total de TLV LLDP reçus de type 802.1.
TLV 802,3	Nombre total de TLV LLDP reçus de type 802.3.
TLV UPOE	Nombre total de TLV LLDP reçus de type UPOE.
TLV NTGR	Nombre total de TLV LLDP reçus de type NTGR.

Affiche les informations sur le périphérique local LLDP

Vous pouvez afficher des informations sur le périphérique local LLDP, qui sont des informations que le commutateur lui-même, ou une interface du commutateur, annonce.

Pour afficher les informations sur le périphérique local LLDP :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > LLDP > informations sur le périphérique local**.

La page de connexion de l'appareil local s'affiche.

6. Dans le menu **interface**, sélectionnez une interface sur laquelle la transmission des trames LLDP est activée.

7. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

Le tableau suivant décrit les champs en lecture seule de la page.

Table 55 : Informations sur le périphérique local LLDP

Champ	Description
Sous-type de l'ID du châssis	L'identifiant du commutateur est l'adresse MAC du commutateur (voir le champ suivant).
ID du châssis	Détecter l'adresse MAC du switch
Sous-type de l'ID de port	L'identificateur de port est l'adresse MAC de l'interface (voir le champ suivant).
ID du port	Adresse MAC de l'interface sur le commutateur.
Nom du système :	Le nom du système, le cas échéant, du commutateur.
Description du système	Description du commutateur.
Description des ports	Le nom de l'interface, le cas échéant, de l'interface sur le commutateur.
Capacités du système prises en charge	Les capacités du système du commutateur.
Capacités système activées	Capacités système du commutateur activées.
Type d'adresse de gestion	Type de l'adresse IP de gestion du commutateur.
Adresse de gestion	Adresse IP de gestion annoncée du commutateur.

Affiche les informations sur le périphérique distant LLDP

Vous pouvez afficher des informations sur le périphérique distant LLDP, qui sont des informations publiées par le périphérique connecté à une interface.

Pour afficher les informations sur le périphérique distant LLDP :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > LLDP > informations sur le périphérique distant**.

La page informations sur le périphérique distant s'affiche.

6. Dans le menu **interface**, sélectionnez une interface sur laquelle la réception des trames LLDP est activée.

7. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

Le tableau suivant décrit les champs en lecture seule de la page.

Table 56 : Informations sur le périphérique distant LLDP

Champ	Description
ID distant	ID du périphérique distant.
Commutateur - ID	Adresse MAC du périphérique connecté.
Sous-type d'ID de commutateur	L'identifiant du commutateur est l'adresse MAC du périphérique distant (voir le champ précédent).
ID du port	Identifiant associé à l'interface sur le périphérique distant.
Sous-type de l'ID de port	Type de l'identificateur de port sur le périphérique distant.
Nom du système :	Le nom système, le cas échéant, du périphérique distant.
Description du système	Description du périphérique distant.
Description des ports	Le nom de l'interface, le cas échéant, de l'interface sur le périphérique distant.
Capacités du système prises en charge	Fonctionnalités système prises en charge sur le périphérique distant.
Capacités système activées	Fonctionnalités système activées sur le périphérique distant.
Il est temps de vivre	Durée de vie en secondes de l'entrée à distance reçue.
Type d'adresse de gestion	Type de l'adresse IP de gestion du périphérique distant.
Adresse de gestion	Adresse IP de gestion annoncée du périphérique distant.

Afficher l'inventaire des périphériques distants LLDP

L'inventaire LLDP comprend les périphériques détectés par LLDP.

Pour afficher l'inventaire des périphériques distants LLDP :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > LLDP > LLDP > inventaire des périphériques distants**.

La page inventaire des périphériques distants s'affiche.

6. Pour rechercher une interface, entrez le numéro d'interface au format 0/x, x étant le numéro d'interface, dans le champ **interface de recherche** et cliquez sur le bouton **aller**.

Des informations sur l'interface s'affichent.

7. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

Le tableau suivant décrit les champs en lecture seule de la page.

Table 57 : Informations sur l'inventaire des périphériques distants LLDP

Champ	Description
Port	Interface du commutateur sur laquelle les informations LLDP sont reçues.
ID de périphérique distant	ID du périphérique distant.
Adresse de gestion	Adresse de gestion annoncée du périphérique distant.
Adresse MAC	Adresse MAC du périphérique connecté.
Nom du système :	Nom système du périphérique distant.
ID de port distant :	Numéro d'interface du périphérique distant.
Oui.	Type-Length-Value (TLV) Organisationally unique identifier (oui) du périphérique distant.
Sous-type oui	Sous-type de la TLV oui du périphérique distant.

Protocole de découverte de couche de liaison pour les périphériques de point d'extrémité multimédia

LLDP-MED (Link Layer Discovery Protocol for Media Endpoint Discovery) est une amélioration du protocole LLDP qui prend en charge les fonctionnalités suivantes :

- Détection automatique des stratégies LAN (telles que VLAN, priorité de couche 2 et paramètres DiffServ), ce qui permet le réseau plug-and-play.
- Découverte de l'emplacement des périphériques, qui permet la création de bases de données d'emplacement.
- Gestion étendue et automatisée de l'alimentation des terminaux Power over Ethernet.
- La gestion des stocks, qui vous permet de suivre vos périphériques réseau et de déterminer leurs caractéristiques, telles que le fabricant, les versions logicielles et matérielles, et les numéros de série ou d'actif.

Configurez les paramètres globaux LLDP-MED

Vous pouvez spécifier les paramètres LLDP-MED qui sont appliqués globalement au commutateur.

Pour configurer les paramètres globaux LLDP-MED :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > LLDP > LLDP-MED > Configuration globale**.

La page Configuration globale s'affiche.

6. Dans le champ **nombre de répétitions de démarrage rapide**, entrez le nombre de PDU LLDP transmises lorsque le protocole est activé.

La plage est de 1 à 10. La valeur par défaut du nombre de répétitions rapides est 3.

Le champ classe de périphérique affiche la classification MED du commutateur. Le commutateur est un périphérique de connectivité réseau.

Il existe les quatre types de dispositifs MED suivants, dont les trois premiers sont des terminaux :

- **Classe I** : Périphériques génériques, qui incluent des contrôleurs de communication IP.
- **Classe II** : Périphériques multimédia, qui incluent des ponts de conférence.
- **Classe III** : Périphériques de communication, qui incluent les téléphones IP.
- **Classe IV** : Périphériques de connectivité réseau, qui comprennent les commutateurs LAN, les routeurs, les ponts IEEE 802,1 et les points d'accès IEEE 802,11 WiFi.

7. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurer les paramètres de l'interface LLDP-MED

Vous pouvez spécifier des paramètres LLDP-MED qui sont appliqués à une ou plusieurs interfaces.

Pour configurer les paramètres de l'interface LLDP-MED :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > LLDP > LLDP-MED > Configuration de l'interface** .

La page Configuration de l'interface s'affiche.

6. Si une pile est configurée, indiquez si vous souhaitez afficher les interfaces physiques d'un commutateur ou de tous les commutateurs de la pile :

- **ID d'unité pour un commutateur empilé** : Les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.

Si aucune pile de commutateurs n'est configurée, la seule option est l'ID d'unité 1.

- **Tous:** Les interfaces physiques de tous les commutateurs de la pile sont affichées. Si aucune pile de commutateurs n'est configurée, l'option tous n'a aucun effet.

7. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :

- Pour afficher ou effacer les statistiques d'une seule interface, cochez la case associée à l'interface ou saisissez le numéro de l'interface dans le champ **aller à l'interface** et cliquez sur le bouton **aller**.
- Pour configurer plusieurs interfaces avec les mêmes paramètres, cochez la case associée à chaque interface.
- Pour configurer toutes les interfaces avec les mêmes paramètres, cochez la case dans la ligne d'en-tête.

Les deux champs suivants sont en lecture seule :

- Les champs État du lien indiquent si l'interface est active ou inactive.
- Le champ État opérationnel indique si les TLV LLDP-MED sont transférés sur cette interface.

8. Dans le menu **Etat MED**, sélectionnez si le mode LLDP-MED est activé ou désactivé sur l'interface.

La valeur par défaut est Activer.

9. Dans le menu **notification Status**, indiquez si l'interface prend en charge les notifications LLDP-MED.

La valeur par défaut est désactiver.

10. Configurez si les informations suivantes relatives à la valeur TLV (Transmit type Length Value), toutes activées par défaut, sont transmises pour LLDP-MED dans les trames LLDP PDU :

- **Capacités DES MÉDICAMENTS** . Sélectionnez si l'interface peut envoyer les capacités MED dans une trame LLDP.
- **Stratégie réseau** : Sélectionnez si l'interface peut envoyer la stratégie réseau dans une trame LLDP.
- **Identification de l'emplacement** : Sélectionnez si l'interface peut envoyer des informations d'emplacement dans une trame LLDP.
- **MDI-PSE étendu** : Sélectionnez si l'interface peut envoyer des informations PSE (Power Sourcing Equipment) dans une trame LLDP.
- **Informations sur l'inventaire** : Sélectionnez si l'interface peut envoyer des informations d'inventaire dans une trame LLDP.

11. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

12. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Affiche les informations sur le périphérique local LLDP-MED

Vous pouvez afficher des informations sur le périphérique local LLDP-MED, qui sont des informations que le commutateur lui-même, ou une interface du commutateur, annonce.

Pour afficher les informations sur le périphérique local LLDP-MED :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > LLDP > LLDP-MED > informations sur le périphérique local**.

La page de connexion de l'appareil local s'affiche.

6. Dans le menu **interface**, sélectionnez une interface sur laquelle la transmission des trames LLDP-MED est activée.
7. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

Le tableau suivant décrit les champs en lecture seule de la page.

Table 58 : Informations sur le périphérique local LLDP-MED

Champ	Description
Informations sur la stratégie réseau	
Indique si une stratégie réseau TLV est présente dans les trames LLDP-MED transmises.	
Type d'application multimédia	Le type d'application, qui peut être l'un des suivants : • inconnu • signalisation vocale • voix du client • signalisation vocale invité • voix du téléphone logiciel • visioconférence • Vidéo en flux continu • signalisation vidéo Chaque type d'application transmis comprend l'ID VLAN, la priorité, le DSCP, l'état du bit balisé et l'état du bit inconnu. Une interface peut recevoir un ou plusieurs de ces types d'application. Ces informations ne sont affichées que si un TLV de stratégie réseau est transmis.
Identifiant VLAN	ID VLAN transmis.
Priorité	Priorité transmise.
DSCP	Le DSCP transmis.
État de bit inconnu	État de bit inconnu transmis.
État du bit étiqueté	État du bit étiqueté transmis.
Informations sur l'inventaire	
Indique si un TLV d'inventaire est présent dans les trames LLDP-MED transmises.	
Révision matérielle	Version matérielle transmise.
Révision du micrologiciel	Version du micrologiciel transmise.
Révision logicielle	Version du logiciel transmise.
Numéro de série	Numéro de série transmis.
Nom du fabricant :	Nom du fabricant transmis.
Nom du modèle	Nom du modèle transmis.

Table 58 : Informations sur le périphérique local LLDP-MED (A continué)

Champ	Description
ID d'actif	ID d'actif transmis.
Informations sur l'emplacement	
Indique si un TLV d'emplacement est présent dans les trames LLDP-MED transmises.	
Sous-type	Type d'informations de localisation transmises.
Informations sur l'emplacement	Informations d'emplacement transmises.
PoE étendu	
Indique si des informations sur le périphérique PoE sont présentes dans les trames LLDP-MED transmises.	
Type d'appareil	Type de périphérique PoE transmis. Le commutateur peut alimenter PoE, donc informatique est un équipement d'alimentation (PSE).
Source d'alimentation	Type de source d'alimentation transmise.
Priorité d'alimentation	Type de priorité de puissance transmise.
Valeur de puissance	La puissance en watts qui est transmise, c'est-à-dire que l'information est transmise, pas la puissance réelle.

Affiche les informations sur le périphérique distant LLDP-MED

Vous pouvez afficher des informations sur le périphérique distant LLDP-MED, qui sont des informations publiées par le périphérique connecté à une interface.

Pour afficher les informations sur le périphérique distant LLDP-MED :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > LLDP > LLDP-MED > informations sur le périphérique distant**.

La page informations sur le périphérique distant s'affiche.

6. Dans le menu **interface**, sélectionnez une interface sur laquelle la réception des trames LLDP-MED est activée.

Le champ ID distant affiche l'ID attribué au périphérique distant.

7. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

Le tableau suivant décrit les champs en lecture seule de la page.

Table 59 : Informations sur le périphérique distant LLDP-MED

Champ	Description
Informations sur les capacités	
Affiche les capacités prises en charge reçues dans les trames LLDP-MED.	
Fonctionnalités prises en charge	Fonctionnalités système prises en charge sur le périphérique distant.
Fonctionnalités activées	Fonctionnalités système activées sur le périphérique distant.
Classe d'appareil	Classe de périphérique annoncée par le périphérique distant. La classe de périphérique peut être Générique, Média, communication ou connectivité réseau.
Informations sur les stratégies réseau	
Affiche les informations sur les stratégies réseau reçues dans les trames LLDP-MED.	

Table 59 : Informations sur le périphérique distant LLDP-MED (A continué)

Champ	Description
Type d'application multimédia	Le type d'application du périphérique distant, qui peut être l'un des suivants : • inconnu • signalisation vocale • voix du client • signalisation vocale invité • voix du téléphone logiciel • visioconférence • Vidéo en flux continu • signalisation vidéo Chaque type d'application reçu comprend l'ID VLAN, la priorité, le DSCP, l'état du bit balisé et l'état du bit inconnu. Une interface peut recevoir un ou plusieurs de ces types d'application. Ces informations ne s'affichent que si un TLV de stratégie réseau est reçu.
Identifiant VLAN	ID VLAN du périphérique distant.
Priorité	Priorité du périphérique distant.
DSCP	Le DSCP du périphérique distant.
État de bit inconnu	État de bit inconnu du périphérique distant.
État du bit étiqueté	État du bit étiqueté du périphérique distant.
Informations sur l'inventaire	
Affiche les informations d'inventaire reçues dans les trames LLDP-MED.	
Révision matérielle	Version matérielle du périphérique distant.
Révision du micrologiciel	Version du micrologiciel du périphérique distant.
Révision logicielle	Version du logiciel du périphérique distant.
Numéro de série	Numéro de série du périphérique ReadyNAS.
Nom du fabricant :	Nom du fabricant du périphérique distant.
Nom du modèle	Nom de modèle du périphérique distant.
ID d'actif	ID d'actif du périphérique distant.
Informations sur l'emplacement	
Affiche les informations d'emplacement reçues dans les trames LLDP-MED.	
Sous-type	Type d'informations de localisation du périphérique distant.
Informations sur l'emplacement	Informations de localisation du périphérique distant.

Table 59 : Informations sur le périphérique distant LLDP-MED (A continué)

Champ	Description
PoE étendu	
Indique si des informations PoE étendues sont reçues dans des trames LLDP-MED.	
Type d'appareil	Type de périphérique PoE du périphérique distant.
PSE PoE étendu :	
Indique si des informations PoE étendues PSE sont reçues dans des trames LLDP-MED.	
Type d'appareil	Type de périphérique PoE utilisé par le périphérique distant.
Source d'alimentation	Type de source d'alimentation de ce périphérique distant.
Priorité d'alimentation	Type de priorité d'alimentation sur le périphérique distant.
Valeur de puissance	Puissance en watts transmise par l'appareil distant, c'est-à-dire que les informations sont transmises, et non la puissance réelle.
PoE PD étendu :	
Indique si des informations PoE PD étendues sont reçues dans des trames LLDP-MED.	
Type d'appareil	Type de périphérique PoE utilisé par le périphérique distant.
Source d'alimentation	Type de source d'alimentation de ce périphérique distant.
Priorité d'alimentation	Type de priorité d'alimentation sur le périphérique distant.
Valeur de puissance	Puissance en watts transmise par l'appareil distant, c'est-à-dire que les informations sont transmises, et non la puissance réelle.

Afficher l'inventaire des périphériques distants LLDP-MED

L'inventaire LLDP comprend les périphériques détectés par LLDP et prenant en charge MED.

Pour afficher l'inventaire des périphériques distants LLDP-MED :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.
4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **système > LLDP > LLDP-MED > inventaire des périphériques distants**.
La page inventaire des périphériques distants s'affiche.
6. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).
Le tableau suivant décrit les champs en lecture seule de la page.

Table 60 : Informations d'inventaire des périphériques distants LLDP-MED

Champ	Description
Port	Interface du commutateur sur laquelle les informations LLDP-MED sont reçues
Adresse de gestion	Adresse de gestion annoncée du périphérique distant
Adresse MAC	Adresse MAC du périphérique connecté.
Modèle du système	Modèle du système du périphérique distant
Révision logicielle	Version du logiciel exécutée sur le périphérique distant

Dépendance de liens

Dépendance de lien vous permet d'activer ou de désactiver une ou plusieurs interfaces en fonction de l'état de lien d'une ou plusieurs *autres* interfaces. Autrement dit, si vous activez la dépendance de lien sur une interface, l'état de lien de cette interface dépend de l'état de lien d'une autre interface. Par exemple, si le port 0/2 dépend du port 0/4 et que le commutateur détecte une perte de liaison sur le port 0/4, le commutateur

peut arrêter automatiquement la liaison sur le port 0/2. Lorsque la liaison est restaurée sur le port 0/4, le commutateur peut automatiquement restaurer la liaison sur le port 0/2.

L'inverse est également vrai : Si le port 0/2 dépend du port 0/4 et que le commutateur détecte une perte de liaison sur le port 0/4, le commutateur peut automatiquement activer la liaison sur le port 0/2. Lorsque la liaison est restaurée sur le port 0/4, le commutateur peut automatiquement arrêter la liaison sur le port 0/2.

Configurer un groupe de dépendances de liens

Un groupe de dépendance de liaison comprend une liste d'interfaces amont, une liste d'interfaces aval et une action configurée pour le groupe. Si toutes les interfaces en amont de la liste sont désactivées, toutes les interfaces en aval de la liste sont désactivées ou activées, en fonction de l'action que vous configurez pour le groupe de dépendances de liens.

Après avoir configuré le groupe de dépendances de liaisons, configurez les interfaces amont et aval du groupe (voir [Configurer ou afficher les interfaces en amont et en aval pour un groupe de dépendances de liens](#) à la page 298).

Pour configurer un groupe de dépendances de liens :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > dépendance de lien > Configuration du groupe de dépendance de lien**.

La page Link Dependency Group Configuration s'affiche.

6. Cochez une ou plusieurs cases pour les ID de groupe.

Le commutateur prend en charge 16 ID de groupe.

❗ Remarque: Les ID de groupe ne sont pas associés aux numéros d'interface.

7. Dans le menu **Link action**, spécifiez les actions suivantes qui doivent se produire sur les interfaces en aval du groupe lorsque toutes les interfaces en amont du groupe sont hors service :

- **Liaison interrompue** : Lorsque toutes les interfaces en amont du groupe sont hors service, toutes les interfaces en aval du groupe sont également hors service. Lorsque l'une des interfaces amont du groupe est activée, toutes les interfaces aval du groupe sont également activées.
- **Lien vers le haut** : Lorsque toutes les interfaces en amont du groupe sont hors service, toutes les interfaces en aval du groupe sont activées. Lorsque l'une des interfaces en amont du groupe est active, toutes les interfaces en aval du groupe sont désactivées.

8. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurer ou afficher les interfaces en amont et en aval pour un groupe de dépendances de liens

Dans un groupe de dépendances de liens, si vous ajoutez des interfaces en aval au groupe, les interfaces sont arrêtées jusqu'à ce que vous ajoutiez une ou plusieurs interfaces en amont au groupe. Ensuite, l'état de liaison des interfaces en aval est déterminé par l'état de liaison des interfaces en amont et l'action que vous configurez pour le groupe. Nous vous recommandons de configurer d'abord les interfaces en amont, puis les interfaces en aval.

Dans un groupe de dépendance de lien, une interface peut être membre de la liste amont ou de la liste aval, pas les deux.

Pour configurer ou afficher les interfaces amont et aval d'un groupe de dépendances de liens :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > dépendance de liaison > Configuration de l'interface de dépendance de liaison**.

La page Configuration de l'interface de dépendance de liaison s'affiche.

6. Dans la section ID de groupe de dépendance de liaison, dans le menu **ID de groupe**, sélectionnez l'ID de groupe pour lequel vous souhaitez afficher ou configurer les paramètres.

❗ Remarque: Les ID de groupe ne sont pas associés aux numéros d'interface.

7. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :

- **1 ou ID d'unité pour un commutateur empilé :**

- 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
- **ID d'unité pour un commutateur empilé :** Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.

- LAG Seuls les LAG sont affichés.

- **Tous:** Les interfaces physiques et les LAG sont affichés, ou pour une pile de commutateurs, les interfaces physiques de tous les commutateurs de la pile et les LAG sont affichés.

8. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :

- Pour afficher ou effacer les statistiques d'une seule interface, cochez la case associée à l'interface ou saisissez le numéro de l'interface dans le champ **aller à l'interface** et cliquez sur le bouton **aller**.
- Pour configurer plusieurs interfaces avec les mêmes paramètres, cochez la case associée à chaque interface.
- Pour configurer toutes les interfaces avec les mêmes paramètres, cochez la case dans la ligne d'en-tête.

9. Dans le menu **interface en aval**, indiquez si l'interface est membre de la liste en aval du groupe.

- Faux L'interface n'est pas membre de la liste en aval du groupe. Il s'agit de l'option par défaut.
- Vrai L'interface est membre de la liste en aval du groupe.

10. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

11. Dans le menu **interface en amont**, indiquez si l'interface est membre de la liste en amont du groupe.

- Faux L'interface n'est pas membre de la liste amont du groupe. Il s'agit de l'option par défaut.
- Vrai L'interface est membre de la liste ascendante du groupe.

12. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

Le champ État de la liaison indique si la liaison de l'interface ou du lag correspondant est active ou inactive.

13. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

14. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

Le tableau suivant décrit les champs en lecture seule de la section statistiques du groupe de dépendance de liaison.

Table 61 : Lier les informations statistiques du groupe de dépendances

Champ	Description
ID du groupe	ID de groupe. La plage est de 1 à 16.
Lier l'action	Action à effectuer sur les interfaces descendantes lorsque toutes les interfaces de la liste montante sont inactives.
État du groupe	État actuel du groupe.
Transitions de groupe	Le nombre de transitions de groupe.
Heure de la dernière transition	Heure de la dernière transition de groupe.

Effacer toutes les interfaces d'un groupe de dépendances de liens

Vous pouvez effacer toutes les interfaces d'un groupe de dépendances de liens. Après cela, la liste en amont et la liste en aval du groupe n'incluent aucune interface.

Pour effacer toutes les interfaces d'un groupe de dépendances de liens :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > dépendance de liaison > Configuration de l'interface de dépendance de liaison**.

La page Configuration de l'interface de dépendance de liaison s'affiche.

6. Dans la section ID de groupe de dépendance de liaison, dans le menu **ID de groupe**, sélectionnez l'ID de groupe pour lequel vous souhaitez afficher ou configurer les paramètres.

La plage de l'ID de groupe est comprise entre 1 et 16.

❗ Remarque: Les ID de groupe ne sont pas associés aux numéros d'interface.

7. Cliquez sur le bouton **Clear** (Effacer).

Les interfaces sont supprimées du groupe.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Protocole de découverte standard de l'industrie

ISDP (Industry Standard Discovery Protocol) est un protocole qui permet aux périphériques de partager des informations dans un réseau.

Vous pouvez configurer les paramètres globaux et d'interface pour ISDP.

Configurez les paramètres ISDP globaux

Vous pouvez configurer les paramètres ISDP qui s'appliquent globalement au commutateur.

Pour configurer les paramètres ISDP globaux :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > ISDP > basique > Configuration globale**.

La page Configuration globale s'affiche.

6. Sélectionnez le bouton radio mode Admin **désactiver** ou **Activer** pour indiquer si le service ISDP est désactivé ou activé.

La valeur par défaut est Activer.

7. Dans le champ **Timer**, spécifiez la période en secondes entre la transmission des paquets ISDP.

La plage est de 5 à 254 secondes. La valeur par défaut est de 30 secondes.

8. Dans le champ **Hold Time**, spécifiez la durée de conservation des paquets ISDP transmis par le commutateur.
La durée de conservation spécifie la durée pendant laquelle un périphérique récepteur doit stocker les informations envoyées dans le paquet ISDP avant de rejeter informatique. La plage est de 10 à 255 secondes. La valeur par défaut est de 180 secondes.
9. Sélectionnez le bouton radio **activation** ou **désactivation** des annonces version 2 pour spécifier si le commutateur peut envoyer des paquets ISDPv2.
La valeur par défaut est Activer.
10. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
11. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 62 : Informations de configuration globale ISDP

Champ	Description
Dernière modification de la table des voisins	Heure à laquelle les informations de la table voisins ont été modifiées.
ID de périphérique	ID de périphérique de ce commutateur.
Capacité de format d'ID de périphérique	Capacité de format d'ID de périphérique.
Format d'ID de périphérique	Format de l'ID du périphérique.

Configurer les paramètres ISDP d'une interface

Vous pouvez configurer si une interface peut communiquer des paquets IDSP.

Pour configurer les paramètres ISDP d'une interface :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **système > ISDP > Avancé > Configuration de l'interface** .

La page Configuration de l'interface s'affiche.

6. Si une pile est configurée, indiquez si vous souhaitez afficher les interfaces physiques d'un commutateur ou de tous les commutateurs de la pile :

- **ID d'unité pour un commutateur empilé** : Les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
Si aucune pile de commutateurs n'est configurée, la seule option est l'ID d'unité 1.
- **Tous**: Les interfaces physiques de tous les commutateurs de la pile sont affichées.
Si aucune pile de commutateurs n'est configurée, l'option tous n'a aucun effet.

7. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :

- Pour afficher ou effacer les statistiques d'une seule interface, cochez la case associée à l'interface ou saisissez le numéro de l'interface dans le champ **aller à l'interface** et cliquez sur le bouton **aller**.
- Pour configurer plusieurs interfaces avec les mêmes paramètres, cochez la case associée à chaque interface.
- Pour configurer toutes les interfaces avec les mêmes paramètres, cochez la case dans la ligne d'en-tête.

8. Dans le menu **mode Admin**, sélectionnez **Activer** ou **désactiver** pour spécifier si l'interface peut communiquer des informations ISDP.

La valeur par défaut est Activer.

9. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Afficher ou effacer les informations de voisinage ISDP

Vous pouvez afficher ou effacer les informations sur les voisins ISDP.

Pour afficher ou effacer les informations de voisinage ISDP :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur principale à la page 46.
4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **système > ISDP > Avancé > voisin**.
La page voisine s'affiche.

6. Pour rechercher un voisin, dans le menu Rechercher , sélectionnez **ID de périphérique** ou **interface**, et dans le champ , entrez l'ID de périphérique ou le numéro d'interface .
7. Pour actualiser la page journal, cliquez sur le bouton Refresh (Actualiser).
8. Pour effacer les informations de voisinage ISDP, cliquez sur le bouton **Effacer**.
Toutes les informations de la page sont effacées.
9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 63 : Informations de voisinage ISDP

Champ	Description
ID de périphérique	ID de périphérique du voisin ISDP.
Interface	Interface sur laquelle le voisin est découvert.
Adresse	Adresse IP du voisin.
Capacité	La capacité du voisin, qui peut être l'une des suivantes : • Routeur • Pont TRANS • Route source • Switch • Hôte • IGMP • Répéteur
Plate-forme	Type de modèle du voisin.
ID du port	ID de port sur le voisin.
Durée de maintien	Temps de maintien des paquets ISDP transmis par le voisin.
Version de la publicité	Version ISDP envoyée par le voisin.
Heure de la dernière modification de l'entrée	Le temps écoulé depuis la dernière entrée a été modifié.
Version logicielle	Version du logiciel sur le voisin.

Afficher ou effacer les statistiques ISDP

Vous pouvez afficher ou effacer les statistiques ISDP.

Pour afficher ou effacer les statistiques ISDP :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.
4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **système > ISDP > Avancé > statistiques**.
La page statistiques s'affiche.
6. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).
7. Pour effacer les statistiques, cliquez sur le bouton **Effacer**.
Les statistiques sont effacées.
8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 64 : Informations statistiques ISDP

Champ	Description
Paquets ISDP reçus	Paquets ISDPv2 et ISDPv3 reçus sur le commutateur.
Paquets ISDP transmis	Paquets ISDPv2 et ISDPv3 transmis sur le commutateur.

Table 64 : Informations statistiques ISDP (A continué)

Champ	Description
Paquets ISDPv1 reçus	Paquets ISDPv1 reçus sur le commutateur.
Paquets ISDPv1 transmis	Paquets ISDPv1 transmis sur le commutateur.
Paquets ISDPv2 reçus	Paquets ISDPv2 reçus sur le commutateur.
Paquets ISDPv2 transmis	Paquets ISDPv2 transmis sur le commutateur.
En-tête ISDP incorrect	Paquets ISDP avec de mauvais en-têtes reçus sur le commutateur.
Erreur de somme de contrôle ISDP	Paquets ISDP avec erreurs de somme de contrôle reçus sur le commutateur.
Défaillance de la transmission ISDP	Nombre de paquets ISDP que le commutateur n'a pas pu transmettre.
Format ISDP non valide	Nombre de paquets ISDP avec un format non valide reçus par le commutateur.
Table ISDP pleine	Taille de la table ISDP.
Table d'adresses IP ISDP pleine	Taille de la table d'adresses IP ISDP.

4

Configurer les informations de commutation

Ce chapitre aborde les sujets suivants :

- [VLAN](#)
- [Auto-VoIP](#)
- [VLAN automatiques](#)
- [Interface Internet Small Computer System](#)
- [Protocole STP](#)
- [Base de données de transfert multidiffusion](#)
- [Surveillance du protocole de gestion de groupe Internet](#)
- [Surveillance de la découverte de l'écouteur multicast](#)
- [Multicast VLAN Registration](#)
- [Table d'adresse MAC](#)
- [Paramètres des ports](#)
- [Lier les groupes d'agrégation](#)
- [802.1AS synchronisation et synchronisation](#)
- [Protocole d'enregistrement multiple et 802.1Qav](#)
- [Protection contre les boucles](#)

VLAN

L'ajout de la prise en charge du réseau local virtuel (VLAN) à un commutateur de couche 2 offre certains des avantages du pontage et du routage. Comme un pont, un commutateur VLAN transfère le trafic en fonction de l'en-tête de couche 2, qui est rapide, et comme un routeur, il partitionne le réseau en segments logiques, ce qui améliore l'administration, la sécurité et la gestion du trafic multicast.

Par défaut, tous les ports du commutateur se trouvent dans le même domaine de broadcast. Les VLAN séparent électroniquement les ports du même commutateur en domaines de diffusion distincts de sorte que les paquets de diffusion ne soient pas envoyés à tous les ports du commutateur. Lorsque vous configurez un VLAN, les utilisateurs peuvent être regroupés par fonction plutôt que par emplacement physique.

Chaque VLAN d'un réseau se voit attribuer un ID VLAN, qui apparaît dans la balise IEEE 802.1Q dans l'en-tête de couche 2 des paquets transmis sur un VLAN. Une station d'extrémité peut omettre l'étiquette, ou la partie VLAN de l'étiquette, auquel cas le premier port de commutation à recevoir le paquet peut soit le rejeter, soit insérer une étiquette en utilisant son ID VLAN par défaut. Un port peut gérer le trafic pour plusieurs VLAN, mais il ne peut prendre en charge qu'un seul ID VLAN par défaut.

Vous pouvez définir des groupes VLAN à stocker dans la table d'appartenance VLAN. Chaque commutateur peut prendre en charge jusqu'à 1024 VLAN. VLAN 1 est créé par défaut pour être utilisé comme VLAN de gestion, et tous les ports sont affectés en tant que membres par défaut.

Gérez la configuration VLAN sur le commutateur

Vous pouvez ajouter, modifier et supprimer des VLAN, ou réinitialiser toute la configuration VLAN sur le commutateur aux paramètres par défaut.

Ajouter un VLAN

Vous pouvez ajouter plusieurs VLAN pour personnaliser le commutateur pour votre réseau.

Un VLAN interne est réservé par une interface de routage basée sur les ports et est invisible pour l'utilisateur final. Une fois qu'un VLAN interne est alloué par l'interface de routage basée sur le port, le VLAN ne peut pas être affecté à une interface VLAN de routage.

Pour ajouter un VLAN :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > VLAN > basique > Configuration VLAN**.

L'écran VLAN Configuration (Configuration IP) s'affiche.

6. Dans la section Configuration VLAN, spécifiez les paramètres du nouveau VLAN :

- Identifiant VLAN : Spécifiez l'identifiant du nouveau VLAN.

La plage de l'ID VLAN peut être comprise entre 1 et 4093.

- Nom du VLAN Saisissez un nom pour le nouveau VLAN.

Le nom peut comporter jusqu'à 32 caractères, espaces compris.

Par défaut, le nom de l'ID VLAN 1 est par défaut.

❗ Remarque: Lorsque vous ajoutez un VLAN manuellement (comme dans cette procédure), le champ VLAN type affiche toujours statique. Un VLAN créé par enregistrement GVRP utilise initialement un type de dynamique, mais vous pouvez changer informatique en statique (voir [Modifier un VLAN](#) à la page 312). Le type de VLAN par défaut (ID VLAN 1) est toujours par défaut.

7. Cliquez sur le bouton **Add** (Ajouter).
L'VLAN est ajouté.
8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Modifier un VLAN

Vous pouvez modifier le nom d'un VLAN ajouté de manière statique ou dynamique. Pour un VLAN ajouté dynamiquement (par exemple, un VLAN créé par enregistrement GVRP), vous modifiez le type VLAN en statique.

Pour modifier un VLAN :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur principale à la page 46.
4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **commutation > VLAN > basique > Configuration VLAN**.
L'écran VLAN Configuration (Configuration IP) s'affiche.
6. Dans la section Configuration VLAN, cochez la case correspondant à l'ID VLAN.

7. Pour modifier le nom VLAN, dans le champ **nom VLAN**, saisissez un nom pour le nouveau VLAN.

Le nom peut comporter jusqu'à 32 caractères, espaces compris.

8. Pour modifier le type de VLAN de dynamique à statique, dans le menu **rendre statique**, sélectionnez **Activer**.

Un VLAN qui est créé par enregistrement GVRP utilise initialement un type de dynamique, mais vous pouvez changer informatique en statique. Vous ne pouvez pas modifier le type d'un VLAN que vous avez ajouté manuellement. Le type de VLAN par défaut (ID VLAN 1) est toujours par défaut.

9. Cliquez sur le bouton **Apply** (Appliquer).

Vos modifications sont enregistrées.

10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimez un ou plusieurs VLAN

Vous pouvez supprimer un ou plusieurs VLAN dont vous n'avez plus besoin. Vous ne pouvez pas supprimer le VLAN par défaut (VLAN 1).

Pour supprimer un ou plusieurs VLAN :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **commutation > VLAN > basique > Configuration VLAN**.
L'écran VLAN Configuration (Configuration IP) s'affiche.
6. Dans la section Configuration VLAN, cochez les cases correspondant aux ID VLAN.
7. Cliquez sur le bouton **Supprimer**.
Les VLAN sont supprimés.
8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Réinitialisez l'ensemble de la configuration VLAN sur les paramètres par défaut

Vous pouvez réinitialiser tous les paramètres de configuration VLAN sur le commutateur aux paramètres par défaut, à l'exception du paramètre VLAN par défaut (VLAN 1). Les valeurs par défaut définies en usine sont les suivantes :

- Tous les ports sont affectés au VLAN par défaut de 1.
- Tous les ports sont configurés avec un PVID de 1.
- Tous les ports sont configurés sur une valeur « types de trames acceptables » de admettre toutes les trames.
- Tous les ports sont configurés avec le filtrage d'entrée désactivé.
- Tous les ports sont configurés pour transmettre uniquement des trames non marquées.
- GVRP est désactivé sur tous les ports et toutes les entrées dynamiques sont effacées.

Pour rétablir les paramètres par défaut de l'ensemble de la configuration VLAN :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > VLAN > Avancé > Configuration VLAN**.

L'écran VLAN Configuration (Configuration IP) s'affiche.

6. Cochez la case **Réinitialiser la configuration**.

Une fenêtre de confirmation s'affiche.

 **Avertissement:** Si vous sélectionnez ce bouton et confirmez votre sélection, tous les paramètres de configuration VLAN du commutateur sont réinitialisés à leurs valeurs par défaut.

7. Cliquez sur le bouton **OK** (Enregistrer).

Tous les VLAN, à l'exception du VLAN par défaut, sont supprimés.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Modifiez les paramètres d'allocation VLAN internes

Dans la plupart des cas, il n'est pas nécessaire de modifier les paramètres d'allocation VLAN internes.

Pour modifier les paramètres d'allocation VLAN internes :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > VLAN > basique > Configuration VLAN** .

L'écran VLAN Configuration (Configuration IP) s'affiche.

6. Dans le champ **Internal VLAN allocation base**, spécifiez la base d'allocation VLAN pour l'interface de routage.

La plage de base par défaut du VLAN interne est comprise entre 1 et 4093.

7. Sélectionnez le bouton radio Stratégie d'allocation de VLAN interne **croissant** ou **décroissant** pour spécifier la stratégie pour l'allocation de VLAN interne :

- **Croissant** : Les VLAN sont alloués par ordre croissant de 2 à 4093.
- **Décroissant** : Les VLAN sont alloués par ordre décroissant de 4093 à 2.

VLAN 1 est le VLAN par défaut.

8. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Présentation du réseau automatique

La liaison automatique est une fonction qui permet au commutateur d'activer automatiquement le mode liaison sur les liaisons physiques compatibles et les interfaces LAG entre les périphériques partenaires. Une jonction peut transporter tous les VLAN actifs. Par défaut, la fonction réseau automatique est activée sur le commutateur.

Si le commutateur configure automatiquement un port en tant que jonction (c'est-à-dire une jonction automatique), tous les VLAN du commutateur font partie de la jonction, ce qui permet la configuration automatique de tous les VLAN du commutateur et du périphérique partenaire avec lequel la jonction est établie.

Avant de configurer un réseau automatique, le commutateur détecte d'abord les liaisons physiques avec le périphérique partenaire qui prend également en charge la fonction réseau automatique, puis configure automatiquement les ports connectés et capables de former un réseau aux deux extrémités.

Une jonction transporte plusieurs VLAN et accepte les paquets étiquetés et non étiquetés. Généralement, une connexion entre le commutateur et un périphérique partenaire tel qu'un routeur, un point d'accès ou un autre commutateur fonctionne comme une jonction.

Pour que le commutateur forme un réseau automatique avec un périphérique partenaire, les éléments suivants sont requis :

- La fonction de jonction automatique doit être prise en charge et activée globalement sur le commutateur et l'appareil partenaire. (Sur le commutateur NETGEAR, la fonction Auto-Trunk est activée par défaut.)
- Les ports interconnectés du commutateur et du périphérique partenaire doivent être activés. (Sur le commutateur NETGEAR, tous les ports sont activés par défaut.)
- LLDP doit être activé sur les ports interconnectés sur le commutateur et le périphérique partenaire. (Sur le commutateur NETGEAR, LLDP est activé par défaut sur tous les ports.)
- Les ports interconnectés sur le commutateur et le périphérique partenaire doivent être en mode port de commutateur par défaut, qui est le mode général. Si les ports sont en mode accès ou déjà en mode réseau, un réseau automatique ne peut pas être formé sur un LAG automatique.

Pour un réseau automatique, le PVID est automatiquement défini sur le VLAN par défaut. Si vous souhaitez modifier le PVID d'un réseau automatique, modifiez le VLAN par défaut.

La fonction Auto-Trunk fonctionne conjointement avec la fonction Auto-LAG (voir). Une fois qu'un LAG automatique est formé, le commutateur applique automatiquement le mode réseau (c'est-à-dire un réseau automatique) au LAG aux deux extrémités. En d'autres termes, après la formation d'un LAG automatique, le mode des ports qui participent à un LAG automatique passe automatiquement du mode de port de commutateur par défaut au mode de port de jonction, et le LAG automatique devient alors un réseau automatique.

Lorsqu'un port ou un LAG automatique devient un réseau automatique, tous les VLAN du commutateur font partie du réseau, et tous les VLAN du commutateur et du périphérique partenaire peuvent être configurés automatiquement.

Activer ou désactiver les lignes de réseau automatiques

Par défaut, la fonction de jonction automatique est activée globalement, mais vous pouvez la désactiver globalement.

Pour activer ou désactiver les lignes de réseau automatiques :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > VLAN > Avancé > Configuration ADF VLAN**.

La page Configuration de VLAN ADF s'affiche.

6. Dans la section mode réseau automatique global, sélectionnez le bouton radio **Activer** ou **désactiver** le mode Admin.

Par défaut, la fonction réseau automatique est activée globalement.

7. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez les paramètres du mode de port de commutateur pour les interfaces

Vous pouvez configurer les paramètres du mode de port de commutateur sur les interfaces. Le mode de port de commutation définit l'objectif du port en fonction du type de périphérique auquel informatique se connecte et limite la configuration VLAN du port en conséquence. L'attribution du mode de port de commutateur approprié permet de simplifier la configuration VLAN et de minimiser les erreurs.

Le commutateur prend en charge les types de ports de commutateur suivants :

- **Accès** Ce mode est destiné aux ports connectés aux périphériques finaux. Les ports d'accès participent à un seul VLAN. Ils acceptent les paquets étiquetés et non étiquetés, mais transmettent toujours des paquets non étiquetés.
- **Général** : Ce mode permet une configuration personnalisée d'un port. Vous pouvez configurer les attributs VLAN généraux du port, tels que l'appartenance (voir [Configurer les interfaces d'appartenance pour un VLAN](#) à la page 322) et le PVID, le balisage, le filtre d'entrée, etc. (Voir [Modifiez les paramètres de l'ID VLAN du port](#) à la page 325). Par défaut, tous les ports sont initialement configurés en mode général.
- **Coffre** : Ce mode s'applique aux ports connectés à d'autres commutateurs ou à un routeur. Un port agrégé peut participer à plusieurs VLAN et accepter des paquets étiquetés et non étiquetés.

Dans la procédure suivante, les ports sont appelés interfaces.

Pour configurer les paramètres du mode de port de commutateur pour les interfaces :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > VLAN > Avancé > Configuration ADF VLAN**.

La page Configuration de VLAN ADF s'affiche.

6. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :

- **1 ou ID d'unité pour un commutateur empilé :**
 - 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
 - **ID d'unité pour un commutateur empilé :** Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
- **LAG** Seuls les LAG sont affichés.
- **Tous:** Les interfaces physiques et les LAG sont affichés, ou pour une pile de commutateurs, les interfaces physiques de tous les commutateurs de la pile et les LAG sont affichés.

7. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :

- Pour afficher ou effacer les statistiques d'une seule interface, cochez la case associée à l'interface ou saisissez le numéro de l'interface dans le champ **aller à l'interface** et cliquez sur le bouton **aller**.
- Pour configurer plusieurs interfaces avec les mêmes paramètres, cochez la case associée à chaque interface.
- Pour configurer toutes les interfaces avec les mêmes paramètres, cochez la case dans la ligne d'en-tête.

8. Dans le menu **Switch port mode**, sélectionnez l'une des options suivantes :

- **Accès** Sélectionnez ce mode si l'interface est connectée à des périphériques finaux. Les interfaces d'accès ne participent qu'à un seul VLAN. Ils acceptent les

paquets étiquetés et non étiquetés, mais transmettent toujours des paquets non étiquetés.

- **Général** : Sélectionnez ce mode pour pouvoir configurer l'interface. Vous pouvez configurer les attributs VLAN généraux du port, tels que l'appartenance (voir Configurer les interfaces d'appartenance pour un VLAN à la page 322) et le PVID, le balisage, le filtre d'entrée, etc. (Voir Modifiez les paramètres de l'ID VLAN du port à la page 325). Il s'agit de la sélection par défaut.
 - **Coffre** : Sélectionnez ce mode si l'interface est connectée à un autre commutateur ou à un routeur. Une interface de jonction peut participer à plusieurs VLAN et accepter des paquets étiquetés et non étiquetés.
9. Effectuez l'une des opérations suivantes, en fonction de votre sélection à l'étape précédente :
- **Accès** Si vous avez sélectionné **accès** dans le menu **Switch port mode**, dans le menu **Access VLAN ID**, sélectionnez l'VLAN d'accès de l'interface.
 - **Coffre** : Si vous avez sélectionné **Trunk** dans le menu **Switch port mode**, procédez comme suit :
 - a. Dans le menu **Native VLAN ID**, sélectionnez le VLAN natif de l'interface.
 - b. Dans le champ **Trunk Allowed VLANs**, entrez les VLAN dont l'interface peut être membre en mode port de commutation pour le Trunk d'interface
Par défaut, le champ inclut tous les VLAN, même s'ils ne sont pas encore créés. Les ID VLAN sont compris entre 1 et 4093. Utilisez un tiret (-) pour spécifier une plage VLAN ou une virgule (,) pour séparer les ID VLAN dans une liste. Les espaces ne sont pas autorisés. Une valeur nulle efface les VLAN autorisés. Si vous saisissez All, tous les VLAN compris entre 1 et 4093 sont inclus.
10. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
11. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.
- Le tableau suivant décrit les champs en lecture seule de la page.

Champ	Définition
Marquage VLAN natif	S'affiche si le marquage VLAN est activé : • Désactiver : Lorsque le marquage VLAN est activé, si le port de jonction reçoit des trames non marquées, informatique les transmet sur le VLAN natif sans balise VLAN. • Activer. Lorsque le marquage VLAN est désactivé, si le port de jonction reçoit des trames non marquées, informatique inclut l'ID VLAN natif dans la balise VLAN lorsque informatique transfère des trames.
État opérationnel du réseau automatique	S'affiche si le réseau automatique est configuré sur l'interface : • Désactiver : Le réseau automatique n'est pas configuré sur l'interface. • Activer. Le réseau automatique est configuré sur l'interface.
Liste VLAN des membres de la ligne réseau automatique	VLAN membres de la jonction automatique, si une jonction automatique est configurée sur l'interface.

Configurer les interfaces d'appartenance pour un VLAN

Pour configurer les interfaces d'appartenance pour un VLAN :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > VLAN > Avancé > abonnement VLAN**.

La page adhésion à VLAN s'affiche.

Les ports du commutateur (unité 1) sont affichés. Si une pile est configurée, les ports de chaque commutateur empilé (unité 1, unité 2, etc.) sont affichés. En outre, tous les LAG sont affichés, qu'une pile soit configurée ou non.

6. Dans le menu **VLAN ID**, sélectionnez VLAN ID.

7. Pour ajouter ou supprimer tous les ports et LAG simultanément (vous pouvez également les sélectionner individuellement), sélectionnez l'une des options suivantes dans le menu **Group Operation** :

- **DESACTIVER LE MARQUAGE POUR TOUT** Tous les ports et LAG sont ajoutés en tant que membres non étiquetés du VLAN.
- **TOUT MARQUER** Tous les ports et LAG sont ajoutés en tant que membres non étiquetés du VLAN.
- **Tout supprimer** Tous les ports et LAG sont exclus du VLAN

8. Dans la table ports (ou, si une pile est configurée, dans l'une des tables ports), cliquez une, deux ou trois fois sur un port pour configurer l'un des modes suivants :

- **T (marqué) membre** : Le port est ajouté en tant que membre balisé du VLAN.
- **Membre U (non étiqueté)** : Le port est ajouté en tant que membre non balisé du VLAN.
- **Membre exclu** : Par défaut, la sélection est vide, ce qui signifie que le port est exclu du VLAN. Un port exclu peut toujours être ajouté dynamiquement au VLAN via GVRP.

Si une pile est configurée, vous pouvez sélectionner des ports dans plusieurs tables.

9. Dans le tableau lag, cliquez une fois, deux fois ou trois fois sur un lag pour configurer l'un des modes suivants :

- **T (marqué) membre** : Le lag est ajouté en tant que membre balisé du VLAN.
- **Membre U (non étiqueté)** : Le lag est ajouté en tant que membre non balisé du VLAN.
- **Membre exclu** : Par défaut, la sélection est vide, ce qui signifie que le lag est exclu du VLAN. Un lag exclu peut toujours être ajouté dynamiquement au VLAN via GVRP.

10. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

11. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 65 : Adhésion VLAN avancée

Champ	Définition
Nom du VLAN	Le nom du VLAN.
Type de VLAN	Le type de VLAN que vous avez sélectionné : • Par défaut (ID VLAN = 1) : Toujours présent. • Statique Un VLAN que vous avez ajouté manuellement. • Dynamique Un VLAN qui a été créé via l'enregistrement GVRP et que vous n'avez pas converti en statique, et que GVRP peut donc supprimer.

Afficher l'état du VLAN sur le commutateur

Vous pouvez afficher l'état de tous les VLAN configurés.

Pour afficher l'état VLAN sur le commutateur :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **commutation > VLAN > Avancé > État VLAN**.
La page VLAN Status s'affiche.
6. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).
Le tableau suivant décrit les champs en lecture seule de la page.

Table 66 : Etat VLAN

Champ	Définition
Identifiant VLAN	Identifiant VLAN (VID) du VLAN. L'ID VLAN est compris entre 1 et 4093.
Nom du VLAN	Le nom du VLAN. VLAN ID 1 est toujours nommé par défaut.
Type de VLAN	Le type de VLAN que vous avez sélectionné : • Par défaut (ID VLAN = 1) : Toujours présent. • Statique Un VLAN que vous avez ajouté manuellement. • Dynamique Un VLAN qui a été créé via l'enregistrement GVRP et que vous n'avez pas converti en statique, et que GVRP peut donc supprimer.
Interface de routage	Interface associée au VLAN, si le routage VLAN est configuré pour ce VLAN.
Ports membres	Interfaces et LAG membres du VLAN.

Modifiez les paramètres de l'ID VLAN du port

Par défaut, chaque interface se voit attribuer un ID VLAN (PVID) de port égal à 1 car informatique est associé au VLAN par défaut, VLAN ID 1.

Si vous souhaitez modifier le PVID d'une interface, l'interface doit être membre d'au moins un autre VLAN en plus du VLAN par défaut.

Outre le PVID, vous pouvez configurer d'autres paramètres liés au PVID.

Pour configurer le PVID et les paramètres associés au PVID :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > VLAN > Avancé > Configuration PVID port**.

La page Port PVID Configuration s'affiche.

6. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :

- **1 ou ID d'unité pour un commutateur empilé :**
 - 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
 - **ID d'unité pour un commutateur empilé :** Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
- **LAG** Seuls les LAG sont affichés.
- **Tous:** Les interfaces physiques et les LAG sont affichés, ou pour une pile de commutateurs, les interfaces physiques de tous les commutateurs de la pile et les LAG sont affichés.

7. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :

- Pour afficher ou effacer les statistiques d'une seule interface, cochez la case associée à l'interface ou saisissez le numéro de l'interface dans le champ **aller à l'interface** et cliquez sur le bouton **aller**.
 - Pour configurer plusieurs interfaces avec les mêmes paramètres, cochez la case associée à chaque interface.
 - Pour configurer toutes les interfaces avec les mêmes paramètres, cochez la case dans la ligne d'en-tête.
8. Dans le champ **PVID**, spécifiez l'ID VLAN à affecter aux trames non balisées ou à priorité balisées reçues sur cette interface.
- Le numéro par défaut est 1.
9. Dans le champ **membre VLAN**, spécifiez l'ID VLAN ou la liste des VLAN d'une interface membre.
- Les identifiants VLAN vont de 1 à 4093. Le numéro par défaut est 1. Utilisez un tiret (-) pour spécifier une plage ou une virgule (,) pour séparer les ID VLAN dans une liste. Les espaces et les zéros ne sont pas autorisés.
10. Dans le champ **balise VLAN**, spécifiez l'ID VLAN ou la liste des VLAN d'une interface balisée.
- Les identifiants VLAN vont de 1 à 4093. Utilisez un tiret (-) pour spécifier une plage ou une virgule (,) pour séparer les ID VLAN dans une liste. Les espaces et les zéros ne sont pas autorisés. Pour rétablir les valeurs par défaut de la configuration des balises VLAN, utilisez le mot clé **aucun**. Le balisage de port pour le VLAN ne peut être défini que si l'interface est membre de ce VLAN.
11. Dans le menu **types de trames acceptables**, sélectionnez les types de trames pouvant être reçues sur l'interface :
- **VLAN uniquement** : Les trames non marquées et les trames marquées par priorité reçues sur l'interface sont rejetées. Les trames marquées VLAN sont transmises conformément à la spécification VLAN 802.1Q.
 - **Admettre tous** : Les trames non marquées et les trames marquées par priorité reçues sur l'interface sont acceptées et la valeur de l'ID VLAN du port de l'interface est affectée. Les trames marquées VLAN sont transmises conformément à la spécification VLAN 802.1Q.
 - **Admettre non étiqueté seulement** : Les trames non marquées reçues sur l'interface sont acceptées. Les trames marquées VLAN sont transmises conformément à la spécification VLAN 802.1Q.
12. Dans le menu **Ingress Filtering**, sélectionnez l'une des options suivantes :
- Activer. La trame est éliminée si l'interface n'est pas membre du VLAN auquel cette trame est associée. Dans une trame balisée, le VLAN est identifié par l'ID

VLAN dans la balise. Dans une trame non marquée, le VLAN est l'ID VLAN du port de l'interface qui reçoit cette trame.

- Désactiver : Toutes les trames sont transmises conformément à la spécification de pont VLAN 802.1Q. La valeur par défaut est désactiver.

13. Dans le champ **priorité du port**, spécifiez la priorité 802.1p par défaut attribuée aux paquets non étiquetés arrivant au port.

Vous pouvez définir un nombre compris entre 0 et 7.

14. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

15. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 67 : Informations de configuration PVID

Champ	Description
Filtrage d'entrée de courant	Indique si le filtrage d'entrée est activé pour l'interface.
Untagged VLAN :	Nombre de VLAN non balisés dont l'interface est membre.
Tagged VLAN :	Nombre de VLAN balisés dont l'interface est membre.
VLAN interdits	Nombre de VLAN interdits dont l'interface est membre.
VLAN dynamiques	Nombre de VLAN ajoutés dynamiquement dont l'interface est membre.

Configurez un VLAN basé sur MAC

Un VLAN basé sur MAC permet d'attribuer des paquets entrants non étiquetés à un VLAN et de classer le trafic en fonction de l'adresse MAC source du paquet.

Vous définissez un mappage MAC-à-VLAN en configurant une entrée dans la table MAC-à-VLAN. Une entrée est définie par son adresse MAC source et un ID VLAN. Les configurations MAC-à-VLAN sont partagées sur toutes les interfaces (c'est-à-dire qu'il existe une table à l'échelle du système avec les mappages adresse MAC-ID-VLAN).

Lorsque des paquets non étiquetés ou prioritaires arrivent au commutateur et que des entrées existent dans la table MAC-to-VLAN, le commutateur tente de trouver l'adresse MAC source du paquet : Si le commutateur trouve une entrée, l'ID VLAN correspondant est attribué au paquet. Si le paquet est déjà marqué en priorité, informatique conserve cette valeur ; sinon, la priorité est définie sur zéro. L'ID VLAN attribué est vérifié par rapport à la table VLAN : Si le VLAN est valide, le traitement d'entrée sur le paquet continue ; sinon, le paquet est abandonné. Cela implique que vous pouvez configurer manuellement un mappage adresse MAC-VLAN-ID.

Ajoutez une configuration VLAN basée sur MAC

Vous pouvez ajouter un mappage adresse-VLAN-ID, que nous appelons configuration VLAN basée sur MAC.

Pour ajouter une configuration VLAN basée sur MAC :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > VLAN > Avancé > MAC Based VLAN** .

La page MAC Based VLAN s'affiche.

6. Dans le champ **adresse MAC**, saisissez une adresse MAC qui doit être liée à un ID VLAN.

7. Dans le champ **ID VLAN**, spécifiez l'ID VLAN dans la plage de 1 à 4093.

8. Cliquez sur le bouton **Add** (Ajouter).

La configuration VLAN basée sur MAC est ajoutée.

9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimez une configuration VLAN basée sur MAC

Pour supprimer une configuration VLAN basée sur MAC :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > VLAN > Avancé > MAC Based VLAN** .

La page MAC Based VLAN s'affiche.

6. Cochez la case correspondant à la configuration VLAN basée sur MAC

7. Cliquez sur le bouton **Supprimer**.

La configuration VLAN basée sur MAC est supprimée.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurer un VLAN basé sur oui

Vous pouvez utiliser un VLAN basé sur oui pour ajouter automatiquement un VLAN à un port, en fonction de l'interface MAC oui du paquet entrant.

Pour définir un VLAN basé sur l'interface utilisateur oui, configurez un VLAN correspondant à l'interface utilisateur MAC afin que le commutateur apprenne l'adresse MAC dans la table MAC L2. Si l'oui correspond, le port entrant devient membre de l'VLAN basé sur l'oui. Le PVID du port entrant est alors défini sur le VLAN basé sur oui. Lorsque l'entrée MAC expire, le port entrant est supprimé du VLAN basé sur oui.

Ajoutez une configuration VLAN basée sur oui

Vous pouvez ajouter une configuration VLAN basée sur oui.

Pour ajouter une configuration VLAN basée sur oui :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > VLAN > Avancé > oui Based VLAN**.

La page de configuration du VLAN basé sur l'interface utilisateur virtuel s'affiche.

6. Dans le champ **oui**, saisissez une interface oui qui doit être liée à un ID VLAN.
7. Dans le champ **ID VLAN**, spécifiez l'ID VLAN dans la plage de 1 à 128.
8. Cliquez sur le bouton **Add** (Ajouter).

La configuration VLAN basée sur oui est ajoutée.

9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimer une configuration VLAN basée sur oui

Pour supprimer une configuration VLAN basée sur oui :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > VLAN > Avancé > oui Based VLAN**.

La page de configuration du VLAN basé sur l'interface utilisateur virtuel s'affiche.

6. Cochez la case correspondant à la configuration VLAN basée sur oui

7. Cliquez sur le bouton **Supprimer**.

La configuration VLAN basée sur oui est supprimée.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurer un groupe VLAN basé sur le protocole

Vous pouvez utiliser un VLAN basé sur le protocole pour définir des critères de filtrage pour les paquets non balisés. Par défaut, si vous ne configurez pas un VLAN basé sur un port (IEEE 802.1Q) ou basé sur un protocole, les paquets non étiquetés sont attribués au VLAN 1. Vous pouvez remplacer ce comportement en définissant des VLAN basés sur des ports ou des VLAN basés sur des protocoles, ou les deux. Les paquets étiquetés sont toujours gérés conformément à la norme IEEE 802.1Q et ne sont pas inclus dans les VLAN basés sur le protocole.

Si vous affectez une interface à un VLAN basé sur un protocole pour un protocole spécifique, les trames non étiquetées reçues sur l'interface pour ce protocole se voient attribuer l'ID VLAN basé sur le protocole. Les trames non marquées reçues sur l'interface pour d'autres protocoles se voient attribuer l'ID VLAN de port, soit l'ID PVID par défaut (1), soit un ID PVID spécifiquement attribué à l'interface (voir [Modifiez les paramètres de l'ID VLAN du port](#) à la page 325).

Vous définissez un VLAN basé sur un protocole en créant un groupe. Chaque groupe a une relation un-à-un avec un ID VLAN, peut inclure une à trois définitions de protocole et peut inclure plusieurs interfaces. Lorsque vous créez un groupe, vous spécifiez un nom. Un ID de groupe est attribué automatiquement.

Ajoutez un groupe VLAN basé sur le protocole

Vous pouvez ajouter un groupe VLAN basé sur le protocole.

Pour ajouter un groupe VLAN basé sur le protocole :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > VLAN > Avancé > Configuration du groupe VLAN basé sur le protocole** .

La page Configuration du groupe VLAN basé sur le protocole s'affiche.

6. Dans le champ **ID de groupe**, spécifiez un ID numérique.

Vous pouvez entrer un intervalle compris entre 1 et 128.

7. Dans le champ **nom du groupe**, spécifiez un nom pour le nouveau groupe.

Vous pouvez entrer jusqu'à 16 caractères.

8. Dans le champ **Protocole**, spécifiez un ou plusieurs des protocoles suivants à associer au groupe :

- **IP** : IP est un protocole de couche réseau qui fournit un service sans connexion pour la livraison des données.
- **ARP** Le protocole ARP (Address Resolution Protocol) est un protocole de bas niveau qui mappe dynamiquement les adresses de couche réseau aux adresses MAC (Medium Access Control) physiques.
- **IPX** : L'échange de paquets interréseau (IPX) est un protocole de couche réseau de datagrammes sans connexion qui transfère les données sur un réseau.

Séparez les protocoles par une virgule (,). Par exemple, pour spécifier les trois protocoles, entrez ce qui suit : ip,arp,ipx

Vous pouvez également entrer des valeurs hexadécimales ou décimales comprises entre 0x0600(1536) et 0xFFFF(65535).

9. Dans le champ **VLAN ID**, spécifiez l'ID VLAN.

L'ID doit être un nombre compris entre 1 et 4093. Une interface du groupe attribue cet ID VLAN aux paquets non balisés que l'interface reçoit pour les protocoles que vous incluez dans ce groupe.

10. Cliquez sur le bouton **Add** (Ajouter).

Le groupe VLAN basé sur le protocole est ajouté.

Le champ ports affiche les ports d'interface appartenant au groupe.

11. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Modifier un groupe VLAN basé sur le protocole

Vous pouvez modifier un groupe VLAN basé sur le protocole existant.

Pour modifier un groupe VLAN basé sur le protocole :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > VLAN > Avancé > Configuration du groupe VLAN basé sur le protocole**.

La page Configuration du groupe VLAN basé sur le protocole s'affiche.

6. Cochez la case correspondant à l'ID de groupe.

7. Modifier les paramètres est nécessaire.

Pour plus d'informations, consultez [Ajoutez un groupe VLAN basé sur le protocole](#) à la page 333.

8. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimer un groupe VLAN basé sur le protocole

Vous pouvez supprimer un groupe VLAN basé sur un protocole dont vous n'avez plus besoin.

Pour supprimer un groupe VLAN basé sur le protocole :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > VLAN > Avancé > Configuration du groupe VLAN basé sur le protocole**.

La page Configuration du groupe VLAN basé sur le protocole s'affiche.

6. Cochez la case correspondant à l'ID de groupe.

7. Cliquez sur le bouton **Supprimer**.

Le groupe VLAN basé sur le protocole est supprimé.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurer les interfaces d'appartenance pour un groupe VLAN basé sur le protocole

Pour un protocole, une interface ne peut appartenir qu'à un seul groupe VLAN basé sur un protocole. Si vous avez déjà ajouté une interface à un groupe pour IP, vous ne pouvez pas ajouter l'interface à un autre groupe qui inclut également IP, mais vous pouvez ajouter informatique à un nouveau groupe pour IPX.

Pour configurer les interfaces d'appartenance pour un groupe VLAN basé sur le protocole :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **commutation > VLAN > Avancé > appartenance à un groupe VLAN basé sur le protocole** .
La page Protocole Based VLAN Group Membership s'affiche.
Les ports du commutateur (unité 1) sont affichés. Si une pile est configurée, les ports de chaque commutateur empilé (unité 1, unité 2, etc.) sont affichés. En outre, tous les LAG sont affichés, qu'une pile soit configurée ou non.
6. Dans le menu **ID de groupe**, sélectionnez l'ID de groupe VLAN basé sur le protocole.
Le champ nom du groupe affiche le nom du VLAN basé sur le protocole que vous avez sélectionné.
7. Pour afficher les membres actuels du groupe VLAN basé sur le protocole sélectionné, cliquez sur le bouton **Membres actuels**.
Une fenêtre contextuelle affiche les membres.
8. Pour sélectionner des interfaces physiques pour le VLAN, effectuez l'une des opérations suivantes :
 - **Sélectionner toutes les interfaces physiques** : Effectuez l'une des opérations suivantes :
 - **Pas de pile de commutateurs** : Cliquez sur l'icône **ports** au-dessus du tableau ports.
 - **Pile de commutateurs** : Si une pile de commutateurs est configurée, cliquez sur l'icône **ID d'unité** au-dessus du tableau ports du commutateur empilé. L'ID de l'unité est un nombre compris entre 1 et 8, représentant le commutateur dans la pile.
 - **Sélectionner des interfaces physiques individuelles** : Effectuez l'une des opérations suivantes :
 - **Pas de pile de commutateurs** : Dans le tableau ports, cliquez sur un ou plusieurs ports individuellement.
 - **Pile de commutateurs** : Si une pile de commutateurs est configurée, dans le tableau ports du commutateur empilé, cliquez sur un ou plusieurs ports individuellement. Vous pouvez sélectionner des ports dans plusieurs tables ports.
9. Pour sélectionner des LAG pour le VLAN, effectuez l'une des opérations suivantes :

- **Sélectionner tous les LAG** : Cliquez sur l'icône **lag** au-dessus du tableau lag.
- **Sélectionner des LAG individuels** : Dans le tableau lag, cliquez sur un ou plusieurs LAG individuellement.

10. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

11. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez un VLAN basé sur un sous-réseau IP

Vous configurez un mappage de sous-réseau IP à VLAN en spécifiant une adresse IP source, un masque réseau et l'ID VLAN. Les configurations de sous-réseau IP à VLAN sont partagées sur toutes les interfaces du commutateur.

Ajoutez un VLAN basé sur un sous-réseau IP

Vous pouvez ajouter un VLAN basé sur un sous-réseau IP.

Pour ajouter un VLAN basé sur un sous-réseau IP :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > VLAN > Avancé > VLAN basé sur le sous-réseau IP**.

La page VLAN basée sur le sous-réseau IP s'affiche.

6. Dans le champ **adresse IP**, saisissez l'adresse IP.

Saisissez l'adresse IP en notation décimale à points.

7. Dans le champ **masque de sous-réseau**, spécifiez un masque de sous-réseau associé à l'adresse IP.

Entrez le masque de sous-réseau en notation décimale à points.

8. Dans le champ **VLAN ID**, spécifiez l'ID VLAN auquel la configuration IP doit être liée. L'ID VLAN peut être compris entre 1 et 4093.

9. Cliquez sur le bouton **Add** (Ajouter).

Le VLAN basé sur le sous-réseau IP est ajouté.

10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimer un VLAN basé sur un sous-réseau IP

Vous pouvez supprimer un VLAN avancé basé sur un port dont vous n'avez plus besoin.

Pour supprimer un VLAN basé sur un sous-réseau IP :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > VLAN > Avancé > VLAN basé sur le sous-réseau IP**.

La page VLAN basée sur le sous-réseau IP s'affiche.

6. Cochez la case correspondant au VLAN basé sur le sous-réseau IP.

7. Cliquez sur le bouton **Supprimer**.

Le VLAN basé sur le sous-réseau IP est supprimé.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez un double VLAN

Un double VLAN (DVLAN) vous permet de configurer une balise VLAN EtherType dans une balise VLAN. La balise EtherType VLAN peut être une balise 802.1Q, une balise vMAN (Virtual Metropolitan Area Network) ou une balise personnalisée.

Pour configurer l'EtherType global pour le DVLAN et configurer le DVLAN sur une ou plusieurs interfaces :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > VLAN > Avancé > Configuration DVLAN des ports**

La page Port DVLAN Configuration s'affiche.

6. Dans le menu **Global EtherType**, sélectionnez un type de balise qui détermine les 16 premiers bits de la balise DVLAN :

- **Balise 802.1Q** : La balise dot1q qui représente 0x8100.
- **Balise vMAN** : Balise vMAN (Virtual Metropolitan Area Network) qui représente 0x88A8.
- **Balise personnalisée** : Une balise EtherType personnalisée dans la plage de 0 à 65535. Lorsque cette sélection est effectuée, le champ valeur personnalisée s'affiche.

7. Si vous sélectionnez **balise personnalisée** dans le menu **Global EtherType**, entrez la balise personnalisée EtherType dans le champ **valeur personnalisée**.

Le numéro de port doit être compris entre 0 et 65535.

8. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :

- **1 ou ID d'unité pour un commutateur empilé :**
 - 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
 - **ID d'unité pour un commutateur empilé :** Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
 - LAG Seuls les LAG sont affichés.
 - **Tous:** Les interfaces physiques et les LAG sont affichés, ou pour une pile de commutateurs, les interfaces physiques de tous les commutateurs de la pile et les LAG sont affichés.
9. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :
- Pour afficher ou effacer les statistiques d'une seule interface, cochez la case associée à l'interface ou saisissez le numéro de l'interface dans le champ **aller à l'interface** et cliquez sur le bouton **aller**.
 - Pour configurer plusieurs interfaces avec les mêmes paramètres, cochez la case associée à chaque interface.
 - Pour configurer toutes les interfaces avec les mêmes paramètres, cochez la case dans la ligne d'en-tête.
10. Dans le menu **mode Admin**, sélectionnez **Activer** ou **désactiver** pour spécifier si la balise DVLAN sélectionnée est ajoutée aux trames traitées sur l'interface.
- La valeur par défaut est Désactivé et la balise DVLAN sélectionnée n'est pas ajoutée aux trames.
11. Cliquez sur le bouton **Apply** (Appliquer).
- Les paramètres sont enregistrés.
12. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurer un VLAN vocal.

Vous pouvez configurer un VLAN vocal à utiliser avec le trafic vocal. Par exemple, activez le VLAN vocal sur une interface connectée à des téléphones IP. Un VLAN voix peut garantir que la qualité sonore du trafic de téléphone IP reste bonne lorsque le trafic de données sur la même interface est élevé.

Pour configurer un VLAN vocal :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > VLAN > Avancé > Configuration Voice VLAN**.

La page Configuration de Voice VLAN s'affiche.

6. Sélectionnez le bouton radio **désactiver** ou **Activer** le mode Admin pour activer ou désactiver le mode VLAN voix globale sur le commutateur.

La valeur par défaut est désactiver. Si vous souhaitez utiliser un VLAN vocal, vous devez activer le mode VLAN vocal global.

7. Si une pile est configurée, indiquez si vous souhaitez afficher les interfaces physiques d'un commutateur ou de tous les commutateurs de la pile :

- **ID d'unité pour un commutateur empilé** : Les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
Si aucune pile de commutateurs n'est configurée, la seule option est l'ID d'unité 1.
- **Tous** : Les interfaces physiques de tous les commutateurs de la pile sont affichées.
Si aucune pile de commutateurs n'est configurée, l'option tous n'a aucun effet.

8. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :

- Pour afficher ou effacer les statistiques d'une seule interface, cochez la case associée à l'interface ou saisissez le numéro de l'interface dans le champ **aller à l'interface** et cliquez sur le bouton **aller**.
- Pour configurer plusieurs interfaces avec les mêmes paramètres, cochez la case associée à chaque interface.
- Pour configurer toutes les interfaces avec les mêmes paramètres, cochez la case dans la ligne d'en-tête.

9. Dans le menu **mode interface**, sélectionnez le mode Voice VLAN :

- Désactiver : Il s'agit de la valeur par défaut.
- Aucun : Permet à un téléphone IP d'utiliser sa propre configuration pour envoyer du trafic vocal non marqué.
- Identifiant VLAN : Un téléphone IP doit être configuré pour envoyer du trafic vocal balisé.
- Dot1p : Configurer le marquage prioritaire Voice VLAN 802.1p pour le trafic vocal.

Si vous sélectionnez ce mode, entrez la valeur dot1p dans le champ **valeur**.

- Non balisé Un téléphone IP doit être configuré pour envoyer du trafic vocal non balisé.

10. Dans le menu **CS Override mode**, sélectionnez l'une des options suivantes :

- Activer. L'interface ignore (c'est-à-dire remplace) la valeur de priorité 802.1p dans les trames Ethernet que l'informatique reçoit des périphériques connectés. Le champ DSCP remplace la valeur cos.
- Désactiver : L'interface approuve la valeur de priorité dans la trame reçue. La valeur par défaut est désactiver.

11. Dans le menu **Authentication mode**, sélectionnez l'une des options suivantes :

- Activer. Le trafic vocal est autorisé sur une interface VLAN vocale non autorisée. La valeur par défaut est Activer.
- Désactiver : Le trafic vocal n'est autorisé qu'avec une interface VLAN vocale autorisée, pour laquelle dot1x doit être activé (voir [Gérer l'authentification de port sur des ports individuels](#), à la page 903).

12. Dans le champ **valeur DSCP**, configurez la valeur DSCP de l'interface.

La plage est de 0 à 64. Le numéro par défaut est 0.

13. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

Le champ État de fonctionnement affiche l'état de fonctionnement du VLAN vocal sur l'interface.

14. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurer le protocole d'enregistrement d'attribut générique

Le protocole GARP (Generic Attribute Registration Protocol) permet aux périphériques réseau de partager des informations telles que les ID VLAN et l'appartenance à un groupe de multidiffusion sur un réseau local ponté. Autrement dit, les participants GARP peuvent enregistrer et annuler l'enregistrement des valeurs d'attribut dans le LAN. Lorsqu'un participant au GARP déclare ou retire un attribut, la valeur de l'attribut est enregistrée pour cet attribut et pour l'interface à partir de laquelle la déclaration ou le retrait a été effectué.

Ce qui suit s'applique au GARP :

- L'enregistrement se produit uniquement sur les interfaces qui reçoivent une PDU GARP avec une déclaration ou un retrait.
- La désenregistrement se produit uniquement si tous les participants GARP connectés au même segment LAN que l'interface retirent la déclaration.

Configurer les paramètres du commutateur GARP

Vous pouvez activer globalement le protocole GARP VLAN Registration (GVRP) et le protocole GARP Multicast Registration (GMRP) sur le commutateur.

Pour configurer les paramètres du commutateur GARP :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > VLAN > Avancé > Configuration du commutateur GARP**.

La page Configuration du commutateur GARP s'affiche.

6. Sélectionnez le bouton radio GVRP mode **Disable (désactiver)** ou **Activer** le mode GVRP) pour désactiver ou activer le protocole GVRP (GARP VLAN Registration Protocol) globalement pour le commutateur.

Si le protocole GVRP est activé, le commutateur peut partager des ID VLAN avec les périphériques du réseau. La valeur par défaut est désactiver.

7. Sélectionnez le bouton radio GMRP mode **Disable (désactiver)** ou **Activer** le mode GMRP) pour désactiver ou activer le protocole d'enregistrement multidiffusion GARP (GMRP) globalement pour le commutateur.

Si GVMP est activé, le commutateur peut partager des informations de multidiffusion avec les périphériques du réseau. La valeur par défaut est désactiver.

8. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

informatique peut prendre jusqu'à 10 secondes pour que les modifications de configuration GARP prennent effet.

9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez les paramètres GARP pour une ou plusieurs interfaces

Vous pouvez configurer les paramètres GARP pour des interfaces individuelles. Ces réglages prennent effet uniquement si le mode GVRP, le mode GMRP ou les deux modes sont activés sur le commutateur.

Pour configurer les paramètres GARP pour une ou plusieurs interfaces :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > VLAN > Avancé > Configuration du port GARP**.

La page Configuration du port GARP s'affiche.

6. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :

- **1 ou ID d'unité pour un commutateur empilé :**

- 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.

- **ID d'unité pour un commutateur empilé :** Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.

- LAG Seuls les LAG sont affichés.

- **Tous:** Les interfaces physiques et les LAG sont affichés, ou pour une pile de commutateurs, les interfaces physiques de tous les commutateurs de la pile et les LAG sont affichés.

7. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :
 - Pour afficher ou effacer les statistiques d'une seule interface, cochez la case associée à l'interface ou saisissez le numéro de l'interface dans le champ **aller à l'interface** et cliquez sur le bouton **aller**.
 - Pour configurer plusieurs interfaces avec les mêmes paramètres, cochez la case associée à chaque interface.
 - Pour configurer toutes les interfaces avec les mêmes paramètres, cochez la case dans la ligne d'en-tête.
8. Dans le menu **mode GVRP**, sélectionnez **Activer** ou **désactiver** pour spécifier le mode du protocole d'enregistrement GARP VLAN pour le port.

Si vous sélectionnez **désactiver**, le protocole GVRP n'est pas actif et les options heure de jointure, heure de départ et heure de départ sont sans effet. La valeur par défaut est désactiver.
9. Dans le menu **mode GMRP**, sélectionnez **Activer** ou **désactiver** pour spécifier le mode du protocole d'enregistrement de multidiffusion GARP pour le port.

Si vous sélectionnez **désactiver**, le GMRP n'est pas actif et les options heure de jointure, heure de départ et heure de départ sont sans effet. La valeur par défaut est désactiver.
10. Dans le champ **minuterie de jointure**, spécifiez le délai en centisecondes entre la transmission des PDU GARP enregistrant l'appartenance à un groupe VLAN ou multicast.

Entrez un nombre compris entre 10 et 100 (0,1 à 1,0 secondes). La valeur par défaut est de 20 centisecondes (0,2 secondes). Une instance de ce temporisateur existe pour chaque participant GARP pour chaque port.
11. Dans le champ **délai de sortie**, spécifiez le temps d'attente en centisecondes après réception d'une demande d'annulation d'enregistrement pour un groupe VLAN ou multicast avant de supprimer l'entrée associée.

Cela laisse le temps à une autre station d'affirmer l'enregistrement pour le même attribut afin de maintenir un service ininterrompu. Entrez un nombre compris entre 20 et 600 (0,2 à 6,0 secondes). La valeur par défaut est 60 centisecondes (0,6 secondes). Une instance de ce temporisateur existe pour chaque participant GARP pour chaque port.
12. Dans le champ **Leave All Timer**, spécifiez la fréquence (en centisecondes) de génération des PDU LeaveAll.

Une PDU LeaveAll indique que tous les enregistrements seront bientôt désenregistrés. Pour maintenir l'inscription, les participants doivent se joindre à nouveau. La minuterie laisser tout est réglée sur une valeur aléatoire comprise entre LeaveAllTime et 1,5 * LeaveAllTime. La minuterie est spécifiée en centisecondes. Entrez un nombre compris entre 200 et 6000 (2 à 60 secondes). La valeur par défaut

est de 1000 centisecondes (10 secondes). Une instance de ce temporisateur existe pour chaque participant GARP pour chaque port.

13. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

l'ordinateur peut prendre jusqu'à 10 secondes pour que les modifications de configuration GARP prennent effet.

14. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Auto-VoIP

La voix sur protocole Internet (VoIP) permet d'effectuer des appels téléphoniques sur un réseau de données. Comme le trafic vocal est généralement plus sensible au temps que le trafic de données, la VoIP automatique fournit une classification des paquets vocaux afin qu'ils puissent être classés par priorité au-dessus des paquets de données pour une meilleure qualité de service (QoS). Avec Auto-VoIP, la hiérarchisation de la voix est basée sur des protocoles de contrôle d'appel tels que SIP, H.323 et SCCP sur des interfaces ou des bits d'identifiant unique organisationnel (oui).

Configurez les paramètres basés sur le protocole Auto-VoIP.

Pour donner la priorité au trafic vocal dépendant du facteur temps sur le trafic de données, Auto-VoIP basé sur des protocoles détermine si les paquets transportent les protocoles VoIP suivants :

- Protocole SIP (session initiation Protocol)
- H.323
- Pièce de contrôle de connexion de signalisation (SCCP)

Les paquets VoIP qui arrivent sur une interface sur laquelle Auto-VoIP est activé sont marqués avec la valeur de classe de trafic cos spécifiée.

Pour configurer les paramètres basés sur le protocole pour une ou plusieurs interfaces :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > Auto-VoIP > basé sur le protocole > Paramètres de port**.

La page Paramètres du port s'affiche.

6. Dans la section Paramètres globaux basés sur le protocole, spécifiez les paramètres globaux suivants :

- a. Dans le menu **type de priorisation**, sélectionnez **classe de trafic** ou **Remarque**. Ceci spécifie le type de hiérarchisation.

- b. Dans le menu **Class Value**, spécifiez la valeur de classe cos à réaffecter pour les paquets que le VLAN vocal reçoit.

Vous pouvez sélectionner une valeur comprise entre 0 et 6.

Dans la section Paramètres globaux basés sur le protocole, spécifiez les paramètres VoIP automatique pour les interfaces, décrits dans les étapes suivantes.

7. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :

- **1 ou ID d'unité pour un commutateur empilé :**

- 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
 - **ID d'unité pour un commutateur empilé** : Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
 - LAG Seuls les LAG sont affichés.
 - **Tous**: Les interfaces physiques et les LAG sont affichés, ou pour une pile de commutateurs, les interfaces physiques de tous les commutateurs de la pile et les LAG sont affichés.
8. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :
- **Pour configurer une interface unique, cochez la case associée au port ou tapez le numéro de port (par exemple g1) dans le champ aller à l'interface et cliquez sur le bouton aller.**
 - Pour configurer plusieurs interfaces avec les mêmes paramètres, cochez la case associée à chaque interface.
 - Pour configurer toutes les interfaces avec les mêmes paramètres, cochez la case dans la ligne d'en-tête.
9. Dans le menu **Auto VoIP mode**, sélectionnez pour activer ou désactiver le mode Auto VoIP pour l'interface.
- La VoIP automatique est désactivée par défaut.
10. Cliquez sur le bouton **Apply** (Appliquer).
- Les paramètres sont enregistrés.
- Le champ État opérationnel indique si l'interface est active ou inactive.
11. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez les propriétés auto-VoIP basées sur oui.

Avec la VoIP automatique basée sur l'identifiant unique organisationnel (oui), la priorité vocale est fournie en fonction des bits oui.

Configurez les propriétés auto-VoIP basées sur oui.

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > Auto-VoIP > basé sur oui > Propriétés**.

La page Propriétés s'affiche.

6. Dans le champ **ID VLAN VoIP automatique**, saisissez l'ID VoIP VLAN du commutateur.

Aucun VLAN par défaut n'existe pour la VoIP automatique, vous devez créer un VLAN pour la VoIP automatique.

7. Dans le menu **de priorité basée sur oui**, sélectionnez la priorité basée sur oui du commutateur.

La valeur par défaut est 7.

8. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez les paramètres de l'interface basée sur oui

Vous pouvez configurer les paramètres de l'interface oui.

Pour configurer les paramètres de l'interface oui :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > Auto-VoIP > basé sur oui > Paramètres de port**.

La page Paramètres de port s'affiche.

6. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :

- **1 ou ID d'unité pour un commutateur empilé :**

- 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
 - **ID d'unité pour un commutateur empilé** : Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
 - LAG Seuls les LAG sont affichés.
 - **Tous**: Les interfaces physiques et les LAG sont affichés, ou pour une pile de commutateurs, les interfaces physiques de tous les commutateurs de la pile et les LAG sont affichés.
7. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :
- **Pour configurer une interface unique, cochez la case associée au port ou tapez le numéro de port (par exemple g1) dans le champ aller à l'interface et cliquez sur le bouton aller.**
 - Pour configurer plusieurs interfaces avec les mêmes paramètres, cochez la case associée à chaque interface.
 - Pour configurer toutes les interfaces avec les mêmes paramètres, cochez la case dans la ligne d'en-tête.
8. Dans le menu **Auto VoIP mode**, sélectionnez pour activer ou désactiver le mode Auto VoIP pour l'interface.
- La VoIP automatique est désactivée par défaut.
9. Cliquez sur le bouton **Apply** (Appliquer).
- Les paramètres sont enregistrés.
- Le champ État opérationnel indique si l'interface est active ou inactive.
10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Gérer la table oui .

Les fabricants de matériel de périphérique peuvent inclure une interface utilisateur oui dans une carte réseau pour aider à identifier un périphérique matériel. L'oui est un numéro unique de 24 bits attribué par l'autorité d'enregistrement IEEE. Le commutateur est livré préconfiguré avec les oui suivants qui identifient le fabricant du téléphone IP :

- 00:01:E3: SIEMENS
- 00:03:6B: CISCO1
- 00:12 CISCO2
- 00 0F/E2. H3C

- 00:60:B9: NITSUKO
- 00 D0/1E. PINTEL
- 00:E0:75: VERILINK
- 00 :E0 :BB : 3COM
- 00:04:0D: AVAYA1
- 00:1B:4F: AVAYA2
- 00:04 SNOM

Vous pouvez sélectionner une oui existante ou ajouter une nouvelle oui et une description pour identifier les téléphones IP sur le réseau.

Ajoutez un préfixe oui

Vous pouvez ajouter un préfixe oui à la table oui.

Pour ajouter un préfixe oui :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > Auto-VolP > basé sur oui > table oui** .

La page table oui s'affiche.

6. Dans le champ **téléphone oui(s)**, spécifiez le nouveau préfixe VoIP oui au format AA:BB:CC.

La table peut inclure jusqu'à 128 oui.

7. Dans le champ **Description**, entrez la description de l'oui.

La longueur maximale autorisée est de 32 caractères.

8. Cliquez sur le bouton **Add** (Ajouter).

L'entrée oui de téléphonie est ajoutée.

9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimez un ou plusieurs préfixes oui

Vous pouvez supprimer les préfixes oui dont vous n'avez plus besoin.

Pour supprimer un ou plusieurs préfixes oui :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > Auto-VoIP > basé sur oui > table oui**.

La page table oui s'affiche.

6. Cochez la case en regard de chaque préfixe oui à supprimer.

7. Cliquez sur le bouton **Supprimer**.

Les entrées oui de téléphonie sont supprimées.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Afficher l'état Auto-VoIP.

Pour afficher l'état Auto-VoIP :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > Auto-VoIP > Statut Auto-VoIP**.

La page Statut VoIP automatique s'affiche.

6. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

Le tableau suivant décrit les champs en lecture seule de la page.

Table 68 : Informations sur l'état de la VoIP automatique

Champ	Description
ID VLAN VoIP automatique	ID VLAN VoIP automatique.
Nombre maximal de canaux voix pris en charge	Nombre maximal de canaux voix pris en charge.
Nombre de canaux voix détectés	Le nombre de canaux VoIP prioritaires avec succès.

VLAN automatiques

Un VLAN automatique permet à un périphérique d'être automatiquement placé dans un VLAN en fonction du type de périphérique ou du type de trafic qui est typique pour le périphérique. Vous pouvez définir la priorité du niveau de qualité de service (QoS) adapté au type de périphérique pris en charge par VLAN.

Le commutateur est livré préconfiguré avec les auto-VLAN suivants, qui sont désactivés par défaut :

- **Caméra automatique** Le commutateur peut placer les appareils photo détectés dans le VLAN de caméra automatique.
- **WiFi automatique** Le commutateur peut placer les périphériques WiFi détectés dans le VLAN Auto-WiFi.

La hiérarchisation est basée sur des bits d'identifiant unique organisationnel (oui) basés sur le protocole. Par défaut, aucune interface utilisateur n'est configurée pour le VLAN automatique de caméra et le VLAN automatique de WiFi.

Activer et configurer un VLAN de caméra automatique

Vous pouvez activer un VLAN de caméra automatique et configurer la priorité.

Pour activer et configurer un VLAN de caméra automatique :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > Auto-VLAN > Auto-caméra > Configuration globale**

La page Auto-Camera Global Configuration s'affiche.

6. Sélectionnez le bouton radio désactiver ou Activer le mode EEE.

Indique si la fonction Auto-Camera est activée sur le commutateur. Par défaut, la fonction Auto-Camera est désactivée.

7. Dans le champ **VLAN ID**, saisissez l'ID du VLAN qui doit fonctionner comme VLAN de caméra automatique.

8. Dans le menu **priorité**, sélectionnez la priorité pour le trafic sur le VLAN de caméra automatique.

Vous pouvez sélectionner une valeur comprise entre **0** et **7**. La valeur par défaut est 7.

9. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

La page affiche le nombre de périphériques (canaux de caméra) actifs sur le VLAN de caméra automatique.

Configurez une interface en tant que membre de l'VLAN de caméra automatique

Vous pouvez configurer une interface en tant que membre du VLAN de caméra automatique.

Pour configurer une interface en tant que membre du VLAN de caméra automatique :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > Auto-VLAN > Auto-Camera > Configuration de l'interface**.

La page Configuration de l'interface de la caméra automatique s'affiche.

6. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :

- **1 ou ID d'unité pour un commutateur empilé :**

- 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
 - **ID d'unité pour un commutateur empilé** : Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
 - LAG Seuls les LAG sont affichés.
 - **Tous**: Les interfaces physiques et les LAG sont affichés, ou pour une pile de commutateurs, les interfaces physiques de tous les commutateurs de la pile et les LAG sont affichés.
7. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :
- Pour configurer une interface unique, cochez la case associée à l'interface ou saisissez le numéro de l'interface dans le champ **Rechercher** et cliquez sur le bouton **aller**.
 - Pour configurer plusieurs interfaces avec les mêmes paramètres, cochez la case associée à chaque interface.
 - Pour configurer toutes les interfaces avec les mêmes paramètres, cochez la case dans la ligne d'en-tête.
8. Dans le menu **mode Admin**, sélectionnez **désactiver** ou **Activer**.
Cette sélection active ou désactive le mode d'administration de la caméra automatique VLAN sur l'interface. La valeur par défaut est désactiver.
9. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
Le champ Operational (fonctionnement) indique si l'interface est active (haut ou bas).

Ajoutez une interface utilisateur oui pour l'Auto-Camera VLAN

L'oui est un identifiant unique pour le fabricant ou le fournisseur d'un périphérique. L'oui est spécifié en trois valeurs d'octet avec deux-points, et chaque octet est représenté par deux chiffres hexadécimaux.

Vous pouvez ajouter une nouvelle interface utilisateur oui et une description pour identifier une caméra sur le réseau. Le commutateur prend en charge un total de 256 oui pour les VLAN Auto-Camera et Auto-WiFi combinés.

Pour ajouter une interface utilisateur oui pour le VLAN de caméra automatique :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > Auto-VLAN > Auto-Camera > table oui**.

La page Auto-Camera oui table s'affiche.

6. Dans le champ **caméra oui**, saisissez l'interface oui.

L'oui doit être au format AA:BB:CC.

7. Dans le champ **Description**, saisissez une description de 32 caractères maximum.

8. Cliquez sur le bouton **Add** (Ajouter).

Vos paramètres sont enregistrés et l'interface utilisateur oui est supprimée.

Supprimez une interface utilisateur oui pour le VLAN de la caméra automatique

Vous pouvez supprimer une interface utilisateur oui dont vous n'avez plus besoin pour le VLAN de l'appareil photo automatique.

Pour supprimer une interface utilisateur oui pour le VLAN de caméra automatique :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > Auto-VLAN > Auto-Camera > table oui**.

La page Auto-Camera oui table s'affiche.

6. Cochez les cases correspondant au contenu.

Vous pouvez cocher plusieurs cases.

7. Cliquez sur le bouton **Supprimer**.

Vos paramètres sont enregistrés et l'interface utilisateur oui est supprimée.

Activer et configurer un VLAN Auto-WiFi

Vous pouvez activer un VLAN Auto-WiFi et configurer la priorité.

Pour activer et configurer un VLAN Auto-WiFi :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > Auto-VLAN > Auto-WiFi > Configuration globale**.

La page Configuration globale Auto-WiFi s'affiche.

6. Sélectionnez le bouton radio désactiver ou Activer le mode EEE.

Indique si la fonction Auto-WiFi est activée sur le commutateur. Par défaut, la fonction Auto-WiFi est désactivée.

7. Dans le champ **VLAN ID**, saisissez l'ID du VLAN qui doit fonctionner comme VLAN Auto-WiFi.

8. Dans le menu **priorité**, sélectionnez la priorité pour le trafic sur le VLAN Auto-WiFi.

Vous pouvez sélectionner une valeur comprise entre **0** et **7**. La valeur par défaut est 7.

9. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

La page affiche le nombre de périphériques (canaux WiFi) actifs sur le VLAN Auto-WiFi.

Configurez une interface en tant que membre du VLAN Auto-WiFi

Vous pouvez configurer une interface en tant que membre du VLAN Auto-WiFi.

Pour configurer une interface en tant que membre du VLAN Auto-WiFi :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > Auto-VLAN > Auto-WiFi > Configuration de l'interface**.

La page Configuration de l'interface Auto-WiFi s'affiche.

6. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :
 - **1 ou ID d'unité pour un commutateur empilé :**
 - 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
 - **ID d'unité pour un commutateur empilé :** Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
 - LAG Seuls les LAG sont affichés.
 - **Tous:** Les interfaces physiques et les LAG sont affichés, ou pour une pile de commutateurs, les interfaces physiques de tous les commutateurs de la pile et les LAG sont affichés.
7. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :
 - Pour configurer une interface unique, cochez la case associée à l'interface ou saisissez le numéro de l'interface dans le champ **Rechercher** et cliquez sur le bouton **aller**.
 - Pour configurer plusieurs interfaces avec les mêmes paramètres, cochez la case associée à chaque interface.
 - Pour configurer toutes les interfaces avec les mêmes paramètres, cochez la case dans la ligne d'en-tête.
8. Dans le menu **mode Admin**, sélectionnez **désactiver** ou **Activer**.

Cette sélection active ou désactive le mode d'administration pour le VLAN Auto-WiFi sur l'interface. La valeur par défaut est désactiver.
9. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

Le champ Operational (fonctionnement) indique si l'interface est active (haut ou bas).

Ajoutez une interface utilisateur oui pour le VLAN Auto-WiFi

L'oui est un identifiant unique pour le fabricant ou le fournisseur d'un périphérique. L'oui est spécifié en trois valeurs d'octet avec deux-points, et chaque octet est représenté par deux chiffres hexadécimaux.

Vous pouvez ajouter une nouvelle interface utilisateur oui et une description pour identifier un périphérique WiFi sur le réseau. Le commutateur prend en charge un total de 256 oui pour les VLAN Auto-Camera et Auto-WiFi combinés.

Pour ajouter une interface utilisateur oui pour le VLAN Auto-WiFi :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > Auto-VLAN > Auto-WiFi > table oui**.

La page Auto-WiFi oui table s'affiche.

6. Dans le champ **WiFi oui**, saisissez l'interface oui.

L'oui doit être au format AA:BB:CC.

7. Dans le champ **Description**, saisissez une description de 32 caractères maximum.

8. Cliquez sur le bouton **Add** (Ajouter).

Vos paramètres sont enregistrés et l'interface utilisateur oui est supprimée.

Supprimez une interface utilisateur oui pour le VLAN Auto-WiFi

Vous pouvez supprimer une interface utilisateur oui dont vous avez plus besoin pour le VLAN Auto-WiFi.

Pour supprimer une interface utilisateur oui pour le VLAN Auto-WiFi :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > Auto-VLAN > Auto-WiFi > table oui**.

La page Auto-WiFi oui table s'affiche.

6. Cochez les cases correspondant au contenu.

Vous pouvez cocher plusieurs cases.

7. Cliquez sur le bouton **Supprimer**.

Vos paramètres sont enregistrés et l'interface utilisateur oui est supprimée.

Affiche des informations sur les périphériques connectés au VLAN Auto-Camera et au VLAN Auto-WiFi

Une fois que vous avez activé le VLAN de caméra automatique, le VLAN WiFi automatique ou les deux, et ajouté des oui, vous pouvez afficher des informations sur les périphériques connectés aux VLAN automatiques.

Pour afficher des informations sur les périphériques connectés au VLAN Auto-Camera et au VLAN Auto-WiFi :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > Auto-VLAN > table de session Auto-VLAN**.

La page Auto-VLAN session table s'affiche.

6. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

Le tableau suivant décrit les champs en lecture seule de la page.

Table 69 : Informations sur la session Auto-VLAN

Champ	Description
Interface	Interface à laquelle la caméra ou le périphérique WiFi est connecté
Adresse MAC	Adresse MAC de l'appareil photo ou du périphérique WiFi
Auto-VLAN type	Le type d'Auto-VLAN, soit Auto-Camera VLAN ou Auto-WiFi VLAN

Interface Internet Small Computer System

La fonction iSCSI (Internet Small Computer System interface) peut vous aider à suivre le trafic iSCSI entre les initiateurs iSCSI et les systèmes cibles, généralement des systèmes de stockage tels que les systèmes NAS (Network-Attached Storage) et SAN (Storage Area Network).

Le commutateur surveille ou surveille le trafic pour détecter les paquets utilisés par les périphériques iSCSI lors de l'établissement de sessions et de connexions iSCSI. Les données de ces échanges sont utilisées pour créer des règles de classification qui attribuent le trafic entre les unités à une classe de trafic configurée. Les paquets dans le flux sont mis en file d'attente et planifiés pour la sortie sur le port de destination en fonction de ces règles.

Dans un réseau qui inclut des initiateurs et des cibles iSCSI, iSCSI peut surveiller les sessions iSCSI ou accorder au trafic iSCSI un traitement de qualité de service (QoS) préférentiel. Les règles de classification générées dynamiquement sont utilisées pour diriger le trafic de données iSCSI vers des files d'attente que vous pouvez attribuer à d'autres données transitant par le commutateur. Cela peut empêcher les interruptions de session pendant les périodes d'encombrement qui entraîneraient la perte de paquets iSCSI. Cependant, dans les systèmes où une grande partie du trafic est iSCSI, informatique peut également interférer avec d'autres trafics du plan de contrôle du réseau, tels que ARP ou LACP. Cela signifie que vous devez équilibrer le traitement préférentiel du trafic iSCSI avec les exigences des autres données critiques du réseau.

Vous pouvez afficher et gérer l'optimisation iSCSI en accordant un traitement QoS spécial au trafic entre un initiateur iSCSI et un système cible.

En outre, l'activation de la fonction de *remarque* entraîne la mise à jour des paquets avec les valeurs IEEE 802,1 ou IP-DSCP. Le marquage des paquets avec des données prioritaires fournit un traitement QoS spécial lorsque les paquets circulent sur le réseau.

Activez iSCSI et configurez les paramètres QoS pour le trafic iSCSI

Par défaut, iSCSI est désactivé et le commutateur n'optimise pas le trafic iSCSI. Vous pouvez activer iSCSI et configurer les paramètres QoS pour le trafic iSCSI.

Pour activer iSCSI et configurer les paramètres QoS pour le trafic iSCSI :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > iSCSI > basique > Configuration globale**.

La page Configuration globale iSCSI s'affiche.

6. Sélectionnez un bouton radio d'état iSCSI :

- **Activer** : iSCSI est activé pour le commutateur.
- **Désactiver** : iSCSI est désactivé pour le commutateur. Il s'agit de l'option par défaut.

7. Sélectionnez un bouton radio profil QoS et les paramètres associés :
 - **Balise de priorité VLAN** : les flux iSCSI sont affectés à la balise de priorité VLAN la plus élevée. Dans le menu **Priority Tag (balise de priorité VLAN)**, sélectionnez une balise de priorité comprise entre 0 (priorité la plus basse) et 7 (priorité la plus élevée). La balise par défaut est 5.
 - **DSCP** : les flux iSCSI sont mappés sur la valeur DSCP la plus élevée qui n'est pas utilisée pour la gestion des commutateurs ou un VLAN vocal. Dans le menu **DSCP**, sélectionnez une valeur DSCP comprise entre 0 et 63. Plus la valeur est élevée, plus la priorité est élevée. La valeur par défaut est 46.
8. Sélectionnez un bouton radio Remarque :
 - **Désactiver** : les trames iSCSI qui quittent le commutateur *ne* sont pas marquées par la balise de priorité VLAN configurée ou la valeur DSCP.
 - **Enable** : les trames iSCSI qui quittent le commutateur sont marquées (c'est-à-dire *marquées*) avec la balise de priorité VLAN configurée ou la valeur DSCP. Il s'agit de l'option par défaut.
9. Dans le champ **délai de vieillissement iSCSI**, entrez le nombre de minutes après lequel une session inactive est terminée.

La plage est de 1 minutes à 43200 minutes. La valeur par défaut est 10 minutes.
10. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.
11. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Ajoutez une cible iSCSI

Vous pouvez ajouter une cible iSCSI telle qu'un système NAS ou SAN en attribuant un port cible, une adresse IP de port ou une combinaison des deux, et en attribuant un nom à la cible.

Pour ajouter une cible iSCSI :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.
4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **commutation > iSCSI > Avancé > cibles iSCSI** .
La page iSCSI Targets Configuration s'affiche.
6. Dans le champ **Port TCP**, entrez un port TCP.
Il s'agit d'un numéro de port TCP utilisé pour une cible iSCSI. Vous pouvez ajouter jusqu'à 16 numéros de port TCP.
Par défaut, les ports iSCSI 860 et 3260 sont préconfigurés.
7. Dans le champ **adresse IP**, entrez l'adresse IPv4 de la cible iSCSI.
8. Dans le champ **nom de la cible**, entrez un nom pour la cible iSCSI.
Le nom peut comporter jusqu'à 233 caractères.
9. Cliquez sur le bouton **Add** (Ajouter).
Les paramètres sont enregistrés. La cible iSCSI est ajoutée.
10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Afficher les sessions iSCSI

Vous pouvez afficher des informations sur les sessions iSCSI actives.

Pour afficher les sessions iSCSI :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > iSCSI > Avancé > sessions**.

La page sessions iSCSI s'affiche. Si aucune session n'est présente, la page affiche *aucune session iSCSI n'est disponible*.

6. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

Le tableau suivant décrit les champs en lecture seule de la page.

Champ	Description
Nom de la cible :	Le nom de la cible.
Nom de l'initiateur	Nom de l'initiateur.
ID de session de l'initiateur (ISID)	Identifiant de session iSCSI. Il s'agit de l'ID qu'un initiateur attribue à son noeud final de session.

Afficher des informations détaillées sur les sessions iSCSI

Vous pouvez afficher des informations détaillées sur les sessions iSCSI actives.

Pour afficher des informations détaillées sur les sessions iSCSI :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > iSCSI > Avancé > sessions détaillées**.

La page iSCSI sessions Detailed s'affiche.

6. Dans le menu **session Index**, sélectionnez une session.

7. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

Le tableau suivant décrit les champs en lecture seule de la page.

Champ	Description
Nom de la cible :	Le nom de la cible.
Nom de l'initiateur	Nom de l'initiateur.
Durée de fonctionnement	Temps en jours, heures, minutes et secondes depuis le début de la session en cours.
Temps de vieillissement (en secondes)	Temps restant en secondes avant l'expiration de la session.

(A continué)

Champ	Description
ID de session de l'initiateur (ISID)	Identifiant de session iSCSI. Il s'agit de l'ID qu'un initiateur attribue à son noeud final de session.
Adresse IP de l'initiateur	Adresse IP de l'initiateur.
Port TCP de l'initiateur	Numéro de port TCP utilisé par l'initiateur. (Plusieurs connexions peuvent exister entre l'initiateur et la cible.)
Adresse IP cible	Adresse IP de la cible.
Port TCP cible	Numéro de port TCP utilisé par la cible. (Plusieurs connexions peuvent exister entre la cible et l'initiateur.)

Protocole STP

Le protocole STP (Spanning Tree Protocol) fournit une topologie arborescente pour toute disposition de périphériques réseau. Le protocole STP fournit également un chemin entre les stations d'extrémité d'un réseau, éliminant ainsi les boucles. STP (également appelé STP « classique ») fournit un chemin unique entre les stations terminales, évitant et éliminant les boucles. Pour plus d'informations sur la configuration des paramètres STP globaux du commutateur, reportez-vous à la section [Configurez les paramètres STP et affichez l'état STP](#), à la page 378.

Le commutateur prend en charge les versions Spanning Tree suivantes :

- **CST** : STP commun. Pour plus d'informations sur la configuration de CST, reportez-vous aux sections [Configurez les paramètres CST et affichez l'état CST](#) à la page 381 et [Configurez les paramètres de l'interface CST](#) à la page 384.
- **MSTP** : Le protocole MSTP (multiple Spanning Tree Protocol) prend en charge plusieurs instances de Spanning Tree pour canaliser efficacement le trafic VLAN sur différentes interfaces. Pour plus d'informations sur la configuration de MSTP, reportez-vous aux sections [Gérer les instances MST](#) à la page 390 et [Configurer et afficher les paramètres d'interface d'une instance MST](#) à la page 394.
- **RSTP** STP rapide. Chaque instance du Spanning Tree se comporte de la manière spécifiée dans IEEE 802.1w, Rapid Spanning Tree (RSTP), avec de légères modifications dans le fonctionnement mais pas dans l'effet final (l'effet principal est la transition rapide du port à l'état de transfert).

La différence entre le RSTP et le STP traditionnel (IEEE 802.1D) réside dans la capacité de configurer et de reconnaître la connectivité duplex intégral et les ports connectés aux stations d'extrémité, ce qui permet une transition rapide du port à l'état de

transfert et la suppression des messages de notification de modification de topologie. Ces caractéristiques sont représentées par les paramètres « pointtopoint » et « edgeport ». MSTP est compatible avec RSTP et STP. informatique se comporte d'une manière appropriée pour les ponts STP et RSTP. Un pont MSTP peut être configuré pour se comporter entièrement comme un pont RSTP ou un pont STP.

- **PVST** : Per-VLAN Spanning Tree (PVST) fournit une instance unique de Spanning Tree pour chaque VLAN. Pour plus d'informations sur la configuration de PVTP, reportez-vous aux sections Configurez les paramètres VLAN PVST/RPVST à la page 399 et Configurez les paramètres d'interface PVST et RPVST à la page 404.
- **RPVST** : Rapid Per-VLAN Spanning Tree (RPVST) fournit une instance unique de Spanning Tree pour chaque VLAN, chaque instance se comportant de la manière spécifiée dans IEEE 802.1w, Rapid Spanning Tree (RSTP). Comparé à PVST, RPVST fournit une convergence Spanning Tree plus rapide en réponse aux modifications de topologie de couche 2.

Pour plus d'informations sur la configuration de RPVTP, reportez-vous aux sections Configurez les paramètres VLAN PVST/RPVST à la page 399 et Configurez les paramètres d'interface PVST et RPVST à la page 404.

- ❗ **Remarque:** Pour que deux ponts se trouvent dans la même région, la version de force doit être 802.1s et leurs noms de configuration, clés de condensé et niveaux de révision doivent correspondre. Pour plus d'informations sur les régions et leur effet sur la topologie du réseau, reportez-vous à la norme IEEE 802.1Q.

Configurez les paramètres STP et affichez l'état STP .

Vous pouvez configurer les paramètres du protocole STP (Spanning Tree Protocol) et afficher l'état STP sur le commutateur.

Pour configurer les paramètres STP et afficher l'état STP :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > STP > basique > Configuration STP**.

L'écran STP Configuration (Configuration IP) s'affiche.

6. Sélectionnez le bouton radio **désactiver** ou **Activer** le mode administrateur Spanning Tree.

Indique si l'opération Spanning Tree est activée sur le commutateur.

7. Sélectionnez l'un des boutons radio **forcer la version du protocole** suivants pour spécifier la version STP que le commutateur doit utiliser :

- IEEE 802.1d Protocole Spanning Tree traditionnel (classique).
- IEEE 802.1w Protocole Rapid Spanning Tree.
- IEEE 802.1s Protocole Spanning Tree multiple .
- **PVST** : Protocole Spanning Tree per-VLAN.
- **RPVST** : Protocole Rapid per-VLAN Spanning Tree.

8. Dans le champ **nom de la configuration**, spécifiez un ID ou un nom qui vous permet d'identifier la configuration.

Le nom peut comporter jusqu'à 32 caractères. La valeur par défaut est l'adresse MAC du commutateur.

9. Dans le champ **niveau de révision de la configuration**, spécifiez un ID qui vous permet d'identifier la configuration.

Par exemple, si vous modifiez la configuration, vous pouvez modifier l'ID dans le champ **niveau de révision de la configuration** afin de pouvoir suivre les différentes configurations. Vous pouvez entrer un ID compris entre 0 et 65535. Le numéro par défaut est 0.

10. Sélectionnez l'un des boutons radio **Forward BPDU While STP Disabled** suivants :

- Désactiver : Les BPDU Spanning Tree ne sont pas transmises si Spanning Tree est désactivé sur le commutateur. La valeur par défaut est désactiver.
- Activer. Les BPDU Spanning Tree sont transmises si Spanning Tree est désactivé sur le commutateur.

11. Sélectionnez l'un des boutons radio **BPDU Guard** suivants :

- Désactiver : La fonction de protection BPDU est désactivée, ce qui correspond au paramètre par défaut.
- Activer. La fonction BPDU Guard est activée et applique les limites du domaine STP pour maintenir la topologie active cohérente et prévisible. Les commutateurs situés derrière les ports de périphérie sur lesquels la protection BPDU STP est activée n'affectent pas la topologie STP globale. A la réception des BPDU, le port sur lequel la protection BPDU est activée passe à l'état désactivé.

12. Sélectionnez l'un des boutons radio **filtre BPDU** suivants :

- Désactiver : La fonction filtre BPDU est désactivée, ce qui correspond au paramètre par défaut.
- Activer. La fonction filtre BPDU est activée et s'applique à tous les ports périphériques opérationnels. Un port Edge dans un état opérationnel se connecte à des hôtes qui abandonnent généralement des BPDU. Si un port périphérique opérationnel reçoit une BPDU, informatique perd son état opérationnel. Si un port sur lequel le filtrage BPDU est activé reçoit des BPDU, le port abandonne les BPDU et reste opérationnel.

13. Sélectionnez l'un des boutons radio **Fast Backbone** suivants :

- Désactivé : La fonction Fast Backbone est désactivée, ce qui correspond au paramètre par défaut.
- Sous tension La fonction Fast Backbone est activée. Si un lien indirect échoue, le commutateur peut automatiquement sélectionner un nouveau lien indirect. Avec PVST, le commutateur n'ignore pas les BPDU inférieures (ce qui se produit avec STP), mais laisse les BPDU expirer sur le port où elles ont été reçues. Ensuite, le commutateur envoie des requêtes de liaison racine sur d'autres ports non désignés. Si le commutateur reçoit une réponse positive, informatique sélectionne une nouvelle liaison indirecte.

14. Sélectionnez l'un des boutons radio **Fast Uplink** suivants :

- Désactivé : La fonction liaison montante rapide est désactivée, ce qui correspond au paramètre par défaut.
- Sous tension La fonction Fast Uplink est activée. Si le port racine principal tombe en panne, le temps de récupération lors de la sélection d'un nouveau port racine est réduit.

15. Si vous avez activé Fast Uplink à l'étape précédente, dans le champ **Max Update Rate**, entrez le taux de mise à jour maximal en paquets par seconde.

Vous entrez de 0 à 32000 paquets par seconde. Le numéro par défaut est 150.

16. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

17. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 70 : Informations sur la configuration et l'état STP

Champ	Description
Configuration STP	
Clé de résumé de configuration	Identifiant de la configuration STP.
Sélecteur de format de configuration	Version du format de configuration pour l'échange de BPDU.
Etat STP	
ID MST	Instance MST (multiple Spanning Tree) ou CST (Common Spanning Tree).
ID VID	ID VLAN (VID).
ID FID	ID de filtrage (FID).

Configurez les paramètres CST et affichez l'état CST

Vous pouvez configurer le protocole CST (Common Spanning Tree) et afficher l'état CST sur le commutateur.

Pour configurer les paramètres CST et afficher l'état CST :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **commutation > STP > Avancé > Configuration CST**.
L'écran CST Configuration (Configuration IP) s'affiche.
6. Dans le champ **Bridge Priority (priorité du pont)**, spécifiez la valeur de priorité du pont pour le Spanning Tree commun (CST) et le Spanning Tree commun et interne (CIST).

La plage est de 0 à 61440. La priorité du pont est un multiple de 4096. La priorité par défaut est 32768.

Lorsque des commutateurs ou des ponts exécutent le protocole STP, une priorité est attribuée à chacun d'eux. Après avoir échangé les BPDU, le commutateur avec la valeur de priorité la plus basse devient le pont racine. Si vous spécifiez une priorité qui n'est pas un multiple de 4096, la priorité est automatiquement définie sur la priorité la plus basse suivante, qui est un multiple de 4096. Par exemple, si vous définissez la priorité sur une valeur comprise entre 0 et 4095, informatique est automatiquement défini sur 0.

7. Dans le champ **Bridge Max Age (secondes)**, spécifiez la période en secondes pendant laquelle un pont attend avant d'implémenter une modification topologique.
La plage est comprise entre 6 et 40 secondes, et la valeur doit être inférieure ou égale aux valeurs suivantes : $(2 * \text{délai d'avance du pont}) - 1$ et supérieur ou égal à $2 * (\text{heure d'ouverture du pont} + 1)$.

La valeur par défaut est de 20 secondes.

❗ Remarque: Le champ Bridge Hello Time (secondes) indique la période fixe en secondes pendant laquelle un pont racine attend entre les messages de configuration. La période fixe est de 2 secondes.

8. Dans le champ **délai de transfert du pont (secondes)**, spécifiez la période en secondes pendant laquelle un pont reste à l'état d'écoute et d'apprentissage avant de transférer des paquets.

La période est comprise entre 4 et 30 secondes et la valeur doit être supérieure ou égale à la valeur suivante : $(\text{Pont Max Age} / 2) + 1$.

La valeur par défaut est de 15 secondes.

9. Dans le champ **Spanning Tree maximum Hops**, spécifiez le nombre maximal de sauts de pont que les informations d'une instance CST particulière peuvent parcourir avant d'être supprimées.

La plage est de 6 à 40 secondes. La valeur par défaut est 20 sauts.

10. Dans le champ **nombre de mises en attente de Tx Spanning Tree**, spécifiez le nombre maximal d'unités BPDU que le pont peut envoyer dans la fenêtre de temps Hello.

La plage est de 1 à 10. Le numéro par défaut est 6.

11. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

12. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 71 : Informations sur l'état CST

Champ	Description
Identifiant de pont	Identifiant de pont pour le CST, qui se compose de la priorité du pont et de l'adresse MAC de base du pont.
Temps écoulé depuis le changement de topologie	Temps en secondes depuis que la topologie du CST a changé.
Nombre de modifications de topologie	Nombre de fois que la topologie a changé pour le CST.
Changement de topologie	Ce champ indique si une modification de topologie est en cours sur un port affecté à l'outil CST. (Vrai ou faux.)
Racine désignée	Identifiant de pont du pont racine, qui se compose de la priorité du pont et de l'adresse MAC de base du pont.
Coût du chemin racine	Coût du chemin vers la racine désignée pour le CST.
Port racine	Port par lequel la racine désignée pour le CST est accessible.
Âge max. (S)	Période en secondes qui s'écoule avant qu'un port de pont enregistre ses informations BPDU de configuration.
Délai avant (s)	Durée en secondes pendant laquelle le pont de port racine retarde le processus de transfert. Cette période est une valeur dérivée.

Table 71 : Informations sur l'état CST (A continué)

Champ	Description
Durée de maintien (s)	Période minimale entre la transmission des BPDU de configuration.
Racine régionale CST	Priorité et adresse MAC de base de la racine régionale CST.
Coût chemin CST	Coût du chemin vers la racine régionale CST.
TC déclenché par port	Le port sur lequel le changement de topologie (TC) est déclenché,

Configurez les paramètres de l'interface CST

Vous pouvez configurer un Spanning Tree commun (CST) et un Spanning Tree interne sur une interface spécifique du commutateur.

Une interface peut être désactivée de manière diagnostique (d-Disable) lorsqu'une condition d'erreur grave se produit pour DOT1. La cause la plus courante est l'inondation de BPDU. Les critères d'inondation sont tels que DOT1S reçoit plus de 15 BPDU dans un intervalle de 3 secondes. (Les autres causes d'une condition d-Disable DOT1S sont très rares.)

Pour configurer les paramètres de l'interface CST :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **commutation > STP > Avancé > Configuration du port CST** .
La page Configuration du port CST s'affiche.
6. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :
 - **1 ou ID d'unité pour un commutateur empilé :**
 - 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
 - **ID d'unité pour un commutateur empilé :** Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
 - **LAG** Seuls les LAG sont affichés.
 - **Tous:** Les interfaces physiques et les LAG sont affichés, ou pour une pile de commutateurs, les interfaces physiques de tous les commutateurs de la pile et les LAG sont affichés.
7. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :
 - **Pour configurer une interface unique, cochez la case associée au port ou tapez le numéro de port (par exemple g1) dans le champ aller à l'interface et cliquez sur le bouton aller.**
 - Pour configurer plusieurs interfaces avec les mêmes paramètres, cochez la case associée à chaque interface.
 - Pour configurer toutes les interfaces avec les mêmes paramètres, cochez la case dans la ligne d'en-tête.
8. Dans le champ **priorité du port**, spécifiez la priorité du port dans le CST.
Spécifiez la priorité du port par multiples de 16. Par exemple, si vous définissez la priorité du port sur une valeur comprise entre 0 et 15, informatique est automatiquement défini sur 0. Si vous définissez la priorité du port sur une valeur comprise entre 16 et (2*16-1), informatique est automatiquement défini sur 16, etc. Le numéro par défaut est 128.
9. Dans le menu **Admin Edge Port**, sélectionnez **Activer** ou **désactiver** pour spécifier si le port fonctionne comme un port Edge dans le CIST.
La valeur par défaut est désactiver.
10. Dans le champ **Port Path Cost**, spécifiez une valeur de coût de chemin pour le port dans le CIST

Le numéro de port doit être compris entre 1 et 200000000. Le numéro par défaut est 0.

11. Dans le menu **coût de chemin de port calculé automatiquement**, sélectionnez **Activer** ou **désactiver** pour spécifier si le coût de chemin externe est calculé automatiquement.

Si la valeur du champ **coût du chemin du port** est nulle et que le coût du chemin est calculé automatiquement, la valeur est basée sur la vitesse de liaison du port.

La valeur par défaut est désactiver.

12. Dans le champ **External Port Path Cost**, spécifiez une valeur de coût de chemin externe pour le port dans le CIST.

Le numéro de port doit être compris entre 1 et 200000000. Le numéro par défaut est 0.

13. Dans le menu **calcul automatique du coût du chemin du port externe**, sélectionnez **Activer** ou **désactiver** pour spécifier si le coût du chemin externe est calculé automatiquement.

Si la valeur du champ **coût du chemin du port externe** est nulle et que le coût du chemin externe est calculé automatiquement, la valeur est basée sur la vitesse de liaison du port.

La valeur par défaut est désactiver.

14. Dans le menu **filtre BPDU**, sélectionnez **Activer** ou **désactiver** pour spécifier si le trafic BPDU est filtré sur le port lorsque le protocole STP est activé sur le port.

La valeur par défaut est désactiver.

15. Dans le menu **transfert BPDU**, sélectionnez **Activer** ou **désactiver** pour spécifier si le trafic BPDU arrivant sur le port peut être inondé si le protocole STP est désactivé sur le port.

La valeur par défaut est désactiver.

16. Dans le menu **Edge automatique**, sélectionnez **Activer** ou **désactiver** pour spécifier si le port peut devenir un port Edge si le port ne reçoit pas de BPDU pendant un certain temps.

La valeur par défaut est Activer.

17. Dans le menu **protection racine**, sélectionnez **Activer** ou **désactiver** pour spécifier si le port peut ignorer les informations supérieures reçues par informatique et, de cette façon, protéger la racine du périphérique contre toute modification.

Si vous activez cette option, le port est placé à l'état de rejet et ne transmet aucun paquet. La valeur par défaut est désactiver.

18. Dans le menu **Loop Guard**, sélectionnez **Enable** ou **Disable** pour spécifier si le port est protégé contre les boucles de transfert de couche 2.

Si vous activez cette option, le port passe de l'état « écoute/apprentissage/transfert » à l'état « blocage incohérent de boucle STP ». La valeur par défaut est désactiver.

19. Dans le menu **Garde TCN**, sélectionnez **Activer** ou **désactiver** pour spécifier si le port ne peut pas propager les informations de modification de topologie reçues par informatique.

La valeur par défaut est désactiver.

20. Dans le menu **mode port**, sélectionnez **Activer** ou **désactiver** pour spécifier si le protocole STP est activé ou désactivé sur le port.

La valeur par défaut est désactiver.

21. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

22. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 72 : Informations de configuration du port CST

Champ	Description
Bonjour Timer	Le réglage de la minuterie Hello pour le CST. Par défaut, le paramètre est 2.
Effet de garde BPDU	Indique si un port de périphérie qui reçoit des paquets BPDU est activé ou désactivé.
Etat de redirection de port	Indique l'état STP actuel de l'interface. Si cette option est activée, l'état du port détermine l'action de transfert effectuée sur le trafic. Les états de port possibles sont les suivants : • Désactivé : STP est actuellement désactivé sur l'interface. L'interface transfère le trafic tout en apprenant les adresses MAC. • Bloc : L'interface est actuellement bloquée et ne peut pas être utilisée pour transférer du trafic ou apprendre des adresses MAC. • Ecoute : L'interface est actuellement en mode d'écoute. L'interface ne peut pas transférer le trafic et informatique ne peut pas apprendre les adresses MAC. • Formation : L'interface est actuellement en mode apprentissage. L'interface ne peut pas transférer le trafic. Cependant, informatique peut apprendre de nouvelles adresses MAC. • Suivant : L'interface est actuellement en mode de transfert. L'interface peut transférer le trafic et apprendre de nouvelles adresses MAC. • Transfert manuel : L'interface est actuellement en mode de transfert manuel. L'interface peut transférer le trafic et apprendre de nouvelles adresses MAC.

Affiche l'état de l'interface CST

Vous pouvez afficher les informations d'état CST (Common Spanning Tree) pour les interfaces du commutateur.

Pour afficher l'état de l'interface CST :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > STP > Avancé > Etat du port CST**.

La page Etat du port CST s'affiche.

6. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :

- **1 ou ID d'unité pour un commutateur empilé :**

- 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
- **ID d'unité pour un commutateur empilé** : Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
- LAG Seuls les LAG sont affichés.
- **Tous**: Les interfaces physiques et les LAG sont affichés, ou pour une pile de commutateurs, les interfaces physiques de tous les commutateurs de la pile et les LAG sont affichés.

7. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

Le tableau suivant décrit les champs en lecture seule de la page.

Table 73 : Informations sur l'état de l'interface CST

Champ	Description
Interface	Interface physique ou lag associée à l'outil CST
ID du port	Identificateur de port dans le CST, créé à partir de la priorité de port et du numéro d'interface
Etat de redirection de port	Indique l'état STP actuel de l'interface. Si cette option est activée, l'état du port détermine l'action de transfert effectuée sur le trafic. les états de port possibles sont les suivants : • Désactivé : STP est actuellement désactivé sur l'interface. L'interface transfère le trafic tout en apprenant les adresses MAC. • Bloc. L'interface est actuellement bloquée et ne peut pas être utilisée pour transférer du trafic ou apprendre des adresses MAC. • Ecoute L'interface est actuellement en mode d'écoute. L'interface ne peut pas transférer le trafic et informatique ne peut pas apprendre les adresses MAC. • Formation L'interface est actuellement en mode apprentissage. L'interface ne peut pas transférer le trafic. Cependant, informatique peut apprendre de nouvelles adresses MAC. • Suivant L'interface est actuellement en mode de transfert. L'interface peut transférer le trafic et apprendre de nouvelles adresses MAC. • Transfert manuel : L'interface est actuellement en mode de transfert manuel. L'interface peut transférer le trafic et apprendre de nouvelles adresses MAC
Rôle du port	Chaque port de pont MST activé se voit attribuer un rôle de port pour chaque Spanning Tree. Le rôle de port est l'un des suivants : Racine, désigné, autre, sauvegarde, maître ou Désactivé.
Racine désignée	Pont racine pour le CST, créé à partir de la priorité du pont et de l'adresse MAC de base du pont
Coût désigné	Coût du chemin offert au LAN par le port désigné

Table 73 : Informations sur l'état de l'interface CST (A continué)

Champ	Description
Pont désigné	Identifiant de pont du pont avec le port désigné. Cet identifiant est créé à partir de la priorité du pont et de l'adresse MAC de base du pont.
Port désigné	Identifiant de port sur le pont désigné qui offre le coût le plus bas pour le LAN. Cet identificateur est créé à partir de la priorité du port et du numéro d'interface du port.
Accusé de réception du changement de topologie	Indique si l'indicateur d'accusé de réception de changement de topologie est défini pour la prochaine BPDU à transmettre sur le port (vrai ou faux)
Port de bord	Indique si le port est activé en tant que port périphérique
MAC point à point	L'état point à point, qui indique si la liaison du port est une liaison point à point (vrai) ou non ou (faux)
Racine régionale CST	Identifiant de pont de la racine régionale CST. Cet identifiant est créé à partir de la priorité du pont et de l'adresse MAC de base du pont.
Coût chemin CST	Coût du chemin vers la racine régionale CST
Temps de portage depuis la dernière remise à zéro des compteurs	Heure à laquelle les compteurs ont été effacés pour la dernière fois
État incohérent de la boucle	Indique si l'interface est dans un état de boucle incohérente (faux ou vrai)
Transitions à l'état boucle incohérente	Nombre de fois que l'interface est passée à l'état de boucle incohérente
Transitions hors boucle état incohérent	Nombre de fois que l'interface est sortie de l'état de boucle incohérente

Gérer les instances MST

Vous pouvez ajouter, modifier ou supprimer plusieurs instances de Spanning Tree (MST) sur le commutateur.

L'instance MST se compose d'un ID, d'une valeur de priorité et d'un ID VLAN.

Ajoutez une instance MST et affichez l'état MST

Vous pouvez ajouter une instance MST et afficher l'état MST.

Pour ajouter une instance MST et afficher l'état MST :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > STP > Avancé > Configuration MST**.

L'écran MST Configuration (Configuration IP) s'affiche.

6. Configurez les paramètres de l'instance MST :

- **ID MST** : Dans le champ **ID MST**, spécifiez l'ID du MST. L'ID VLAN peut être compris entre 1 et 4094.
- **Priority** (Priorité). Dans le champ **priorité**, spécifiez la valeur de priorité du pont pour l'instance MST.

Lorsque des commutateurs ou des ponts exécutent le protocole STP, une priorité est attribuée à chacun d'eux. Après avoir échangé les BPDU, le commutateur avec la valeur de priorité la plus basse devient le pont racine. La priorité du pont est un multiple de 4096. Si vous spécifiez une priorité qui n'est pas un multiple de 4096, la priorité est automatiquement définie sur la priorité la plus basse suivante, qui est un multiple de 4096. Par exemple, si vous définissez la priorité sur une valeur comprise entre 0 et 4095, le commutateur définit automatiquement la valeur sur 0. La plage est de 0 à 61440. Le numéro par défaut est 32768.
- Identifiant VLAN : Dans le menu **VLAN ID**, sélectionnez le VLAN qui doit être associé à l'instance MST.

7. Cliquez sur le bouton **Add** (Ajouter).
L'MST est ajouté.
8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.
9. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).
Le tableau suivant décrit les champs en lecture seule de la page.

Table 74 : Informations de configuration MST

Champ	Description
Identificateur de pont	Identificateur de pont pour l'instance MST, créé à l'aide de la priorité de pont et de l'adresse MAC de base du pont.
Dernier TCN	Temps en secondes depuis que la topologie de l'instance MST a changé.
Nombre de modifications de topologie	Nombre de fois que la topologie a changé pour l'instance MST.
Changement de topologie	Ce champ indique si une modification de topologie est en cours sur une interface dans le MST. (Vrai ou faux.)
Racine désignée	Identifiant de pont du pont racine, créé en utilisant la priorité du pont et l'adresse MAC de base du pont
Coût du chemin racine	Coût du chemin vers la racine désignée pour l'instance MST.
Port racine	Port par lequel la racine désignée pour l'instance MST est accessible.

Modifier une instance MST

Vous pouvez modifier une instance MST existante.

Pour modifier une instance MST existante :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > STP > Avancé > Configuration MST**.

L'écran MST Configuration (Configuration IP) s'affiche.

6. Cochez la case associée à l'instance MST.

7. Modifiez les paramètres en fonction de vos besoins.

Pour plus d'informations, consultez [Ajoutez une instance MST et affichez l'état MST](#) à la page 390.

8. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimer une instance MST

Vous pouvez supprimer une instance MST dont vous n'avez plus besoin.

Pour supprimer une instance MST :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > STP > Avancé > Configuration MST**.

L'écran MST Configuration (Configuration IP) s'affiche.

6. Cochez la case associée à l'instance MST.

7. Cliquez sur le bouton **Supprimer**.

L'instance MST est supprimée.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurer et afficher les paramètres d'interface d'une instance MST

Vous pouvez configurer et afficher les paramètres d'interface pour une instance MST (multiple Spanning Tree).

Une interface peut être désactivée de manière diagnostique (d-Disable) lorsqu'une condition d'erreur grave se produit pour DOT1. La cause la plus courante est l'inondation de BPDU. Les critères d'inondation sont tels que DOT1S reçoit plus de 15 BPDU dans un intervalle de 3 secondes. (Les autres causes d'une condition d-Disable DOT1S sont très rares.)

Configurer et afficher les paramètres de port d'une instance MST.

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > STP > Avancé > Configuration du port MST**.

La page Configuration du port MST s'affiche.

6. Dans le menu **sélectionner MST**, sélectionnez une instance MST.

Pour plus d'informations sur l'ajout d'instances MST, reportez-vous à [Gérer les instances MST](#) à la page 390 la section .

7. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :

- **1 ou ID d'unité pour un commutateur empilé :**

- 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
- **ID d'unité pour un commutateur empilé :** Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.

- **LAG** Seuls les LAG sont affichés.

- **Tous:** Les interfaces physiques et les LAG sont affichés, ou pour une pile de commutateurs, les interfaces physiques de tous les commutateurs de la pile et les LAG sont affichés.

8. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :

- **Pour configurer une interface unique, cochez la case associée au port ou tapez le numéro de port (par exemple g1) dans le champ aller à l'interface et cliquez sur le bouton aller.**
- Pour configurer plusieurs interfaces avec les mêmes paramètres, cochez la case associée à chaque interface.
- Pour configurer toutes les interfaces avec les mêmes paramètres, cochez la case dans la ligne d'en-tête.

9. Configurez les valeurs MST pour la ou les interfaces sélectionnées :

- **Priorité des ports** Dans le champ **priorité du port**, spécifiez la priorité de l'interface dans l'instance MST. La priorité du port est définie par multiples de 16. Si vous spécifiez une valeur qui n'est pas un multiple de 16, la priorité est automatiquement définie sur la priorité la plus basse suivante, qui est un multiple de 16. Par exemple, si vous définissez une valeur comprise entre 0 et 15, la priorité est définie sur 0. Si vous spécifiez un nombre compris entre 16 et 31, la priorité est définie sur 16. Spécifiez une valeur comprise entre 0 et 240. Le numéro par défaut est 128.
- **Coût du chemin du port** : Dans le champ **Port Path Cost**, spécifiez le coût du chemin dans la plage de 0 à 200000000. Le numéro par défaut est 0.

10. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

11. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

12. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

Le tableau suivant décrit les champs en lecture seule de la page.

Table 75 : Informations de configuration de l'interface MST

Champ	Description
Coût de chemin de port opérationnel	Coût du chemin utilisé par l'interface
Coût de chemin de port calculé automatiquement	Indique si le coût du chemin est calculé automatiquement (activé) ou non (désactivé). Si cette option est activée, le coût du chemin est calculé en fonction de la vitesse de liaison du port si la valeur configurée pour Port Path Cost est zéro.
ID du port	Identifiant du port dans l'instance MST, créé à l'aide de la priorité du port et du numéro d'interface
Temps de disponibilité du port depuis le dernier effacement des compteurs	Temps écoulé depuis que les compteurs ont été effacés

Table 75 : Informations de configuration de l'interface MST (A continué)

Champ	Description
Mode Port	Indique si le protocole STP est activé pour l'interface
Etat de redirection de port	Indique l'état STP actuel de l'interface. Si cette option est activée, l'état du port détermine l'action de transfert effectuée sur le trafic. les états de port possibles sont les suivants : • Désactivé : STP est actuellement désactivé sur l'interface. L'interface transfère le trafic tout en apprenant les adresses MAC. • Bloc. L'interface est actuellement bloquée et ne peut pas être utilisée pour transférer du trafic ou apprendre des adresses MAC. • Ecoute L'interface est actuellement en mode d'écoute. L'interface ne peut pas transférer le trafic et informatique ne peut pas apprendre les adresses MAC. • Formation L'interface est actuellement en mode apprentissage. L'interface ne peut pas transférer le trafic. Cependant, informatique peut apprendre de nouvelles adresses MAC. • Suivant L'interface est actuellement en mode de transfert. L'interface peut transférer le trafic et apprendre de nouvelles adresses MAC. • Transfert manuel : L'interface est actuellement en mode de transfert manuel. L'interface peut transférer le trafic et apprendre de nouvelles adresses MAC.
Rôle du port	Chaque port de pont MST activé se voit attribuer un rôle de port pour chaque Spanning Tree. Le rôle de port est l'un des suivants : Racine, désigné, autre, sauvegarde, maître ou Désactivé.
Racine désignée	Identifiant de pont du pont racine, créé en utilisant la priorité du pont et l'adresse MAC de base du pont
Coût désigné	Coût du chemin offert au LAN par le port désigné
Pont désigné	Identifiant de pont du pont avec le port désigné. Cet identifiant est créé à partir de la priorité du pont et de l'adresse MAC de base du pont
Port désigné	Identifiant de port sur le pont désigné qui offre le coût le plus bas pour le LAN. Cet identificateur est créé à partir de la priorité du port et du numéro d'interface du port.
État incohérent de la boucle	Indique si l'interface est dans un état de boucle incohérente (faux ou vrai)
Transitions à l'état boucle incohérente	Nombre de fois que l'interface est passée à l'état de boucle incohérente
Transitions hors boucle état incohérent	Nombre de fois que l'interface est sortie de l'état de boucle incohérente

Afficher les statistiques de l'interface STP

Vous pouvez afficher des informations sur le nombre et le type d'unités de données de protocole de pont (BPDU) transmises et reçues sur chaque interface.

Pour afficher les statistiques de l'interface STP :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > STP > Avancé > statistiques STP**.

La page statistiques STP s'affiche.

6. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :

- **1 ou ID d'unité pour un commutateur empilé :**

- 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
 - **ID d'unité pour un commutateur empilé** : Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
 - LAG Seuls les LAG sont affichés.
 - **Tous**: Les interfaces physiques et les LAG sont affichés, ou pour une pile de commutateurs, les interfaces physiques de tous les commutateurs de la pile et les LAG sont affichés.
7. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

Le tableau suivant décrit les champs en lecture seule de la page.

Table 76 : Informations statistiques de l'interface STP

Champ	Description
BPDU STP reçues	Nombre de BPDU STP reçues sur l'interface
BPDU STP transmises	Nombre de BPDU STP transmises depuis l'interface
BPDU RSTP reçues	Nombre de BPDU RSTP reçues sur l'interface
BPDU RSTP transmises	Nombre de BPDU RSTP transmises depuis l'interface
BPDU MSTP reçues	Nombre de BPDU MSTP reçues sur l'interface
BPDU MSTP transmises	Nombre de BPDU MSTP transmises depuis l'interface

Configurez les paramètres VLAN PVST/RPVST

Vous pouvez configurer les paramètres Per-VLAN Spanning Tree Protocol (PVST) et Rapid PVST (RPVST) pour un VLAN.

PVST et RPVST doivent être activés. Pour plus d'informations, consultez [Configurez les paramètres STP et affichez l'état STP](#), à la page 378.

Pour configurer les paramètres VLAN PVST/RPVST pour le commutateur :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > STP > Avancé > VLAN PVST**.

La page VLAN PVST s'affiche.

6. Dans le champ **ID VLAN**, spécifiez un ID VLAN unique.

Vous pouvez spécifier uniquement les VLAN pour lesquels STP est activé et pour lesquels PVST ou RPVST est activé.

7. Dans le menu **racine**, sélectionnez **aucun**, **primaire** ou **secondaire** :

- **Aucun** : La valeur par défaut est aucun. Le commutateur ne fonctionne pas comme un pont racine ou un pont de secours pour le VLAN.
- **Principal** Le commutateur fonctionne comme un pont racine pour le VLAN. La priorité du pont passe de la valeur par défaut de 32768 à une valeur inférieure pour garantir une configuration de pont racine.
- **Secondaire** : Le commutateur fonctionne comme un pont de secours pour le VLAN. La priorité du pont passe de la valeur par défaut de 32768 à une valeur inférieure pour garantir une configuration de pont de secours.

8. Dans le champ **Hello Time**, entrez l'intervalle de temps Hello Spanning Tree pour les VLAN.

L'heure Hello est l'intervalle entre l'envoi de BPDU successives. Entrez une valeur comprise entre 1 et 10 secondes. La valeur par défaut est de 2 secondes.

9. Dans le champ **Forward Time**, entrez l'intervalle de délai de transfert du Spanning Tree pour le VLAN.

Cet intervalle est la période pendant laquelle le commutateur peut détecter un état avant de passer un port d'interface à l'état de transfert. La plage est comprise entre 4 et 30 secondes. La valeur par défaut est de 15 secondes.

10. Dans le champ **Age max.**, entrez la durée d'âge maximum de l'arbre maximal pour le VLAN.

Ce temps est la période après laquelle une interface de pont enregistre ses informations de configuration. La plage est de 6 à 40 secondes. La valeur par défaut est de 20 secondes.

11. Dans le champ **priorité**, entrez la priorité du VLAN.

Les valeurs autorisées sont comprises entre 0 et 61440. Les valeurs valides sont répertoriées dans le tableau suivant.

0	4096	8192
12288	16384	20480
24576	28672	32768 (par défaut)
36864	40960	45056
49152	53248	57344
61440		

La valeur par défaut est 32768. Si la valeur que vous entrez ne fait pas partie des valeurs spécifiées, elle est automatiquement arrondie à la valeur valide la plus proche.

12. Cliquez sur le bouton **Add** (Ajouter).

La configuration VLAN PVST/RPVST est ajoutée.

13. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Modifier une configuration VLAN PVST/RPVST

Vous pouvez modifier une configuration VLAN PVST/RPVST existante.

Pour modifier une configuration VLAN PVST/RPVST existante :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > STP > Avancé > VLAN PVST**.

La page VLAN PVST s'affiche.

6. Cochez la case associée à la configuration PVST/RPVST VLAN.

7. Modifiez les paramètres en fonction de vos besoins.

Pour plus d'informations, consultez [Configurez les paramètres VLAN PVST/RPVST](#) à la page 399.

8. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimer une configuration VLAN PVST/RPVST

Vous pouvez supprimer une configuration VLAN PVST/RPVST dont vous n'avez plus besoin.

Pour supprimer une configuration VLAN PVST/RPVST :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.
4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **commutation > STP > Avancé > VLAN PVST**.
La page VLAN PVST s'affiche.
6. Cochez la case associée à la configuration PVST/RPVST VLAN.
7. Cliquez sur le bouton **Supprimer**.
La configuration PVST/RPVST VLAN est supprimée.
8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez les paramètres d'interface PVST et RPVST

Vous pouvez configurer les paramètres Per-VLAN Spanning Tree Protocol (PVST) et Rapid PVST (RPVST) pour une interface.

PVST et RPVST doivent être activés. Pour plus d'informations, consultez [Configurez les paramètres STP et affichez l'état STP](#), à la page 378.

Pour configurer les paramètres d'interface PVST et RPVST :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > STP > Avancé > interface PVST**.

La page interface PVST s'affiche.

6. Dans le menu **VLAN ID**, sélectionnez un VLAN pour lequel STP et PVST ou RPVST est déjà activé, ou sélectionnez **Other** pour configurer un en saisissant un nouvel ID VLAN.

7. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :

- **1 ou ID d'unité pour un commutateur empilé :**
 - 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
 - **ID d'unité pour un commutateur empilé :** Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
- **LAG** Seuls les LAG sont affichés.
- **Tous:** Les interfaces physiques et les LAG sont affichés, ou pour une pile de commutateurs, les interfaces physiques de tous les commutateurs de la pile et les LAG sont affichés.

8. Dans le champ **priorité**, entrez la priorité de l'interface.

Définissez cette valeur sur un nombre inférieur pour permettre à l'interface de transférer les trames. Priorité s utilisée lorsque l'interface est configurée en tant que liaison point à point. La valeur peut être comprise entre 0 et 240. La valeur doit être un multiple de 16.

0	16	32
48	64	80
96	112	128 (par défaut)
144	160	176
192	208	224
240	-	-

La valeur par défaut est 128. Si la valeur que vous entrez ne fait pas partie des valeurs spécifiées, elle est automatiquement arrondie à la valeur valide la plus proche.

9. Dans le champ **coût**, entrez le coût du chemin de l'interface au pont racine.

Par défaut, le coût n'est pas configuré manuellement. Vous pouvez entrer une valeur comprise entre 1 et 200,000,000. Entrez 0 pour désactiver le paramètre. Si le coût par VLAN n'est pas configuré, la valeur du coût du chemin est définie en fonction de la vitesse de liaison.

10. Dans le menu **coût calculé automatiquement**, sélectionnez **Activer** ou **désactiver** pour spécifier si le coût est calculé automatiquement.

La valeur par défaut est Activer.

11. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

12. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 77 : Informations de configuration de l'interface PVST/RPVST

Champ	Description
Rôle	Rôle de l'interface, qui peut être Désactivé, racine, désigné, alternatif, sauvegarde ou maître Remarque : Pour une interface qui n'est pas membre du VLAN sélectionné, le champ est vide.
Etat	L'état de l'interface, qui peut être en cours, apprentissage, transfert ou Désactivé Remarque : Pour une interface qui n'est pas membre du VLAN sélectionné, le champ est vide.

Afficher les statistiques PVST

Vous pouvez afficher les statistiques PVST (Per-VLAN Spanning Tree Protocol).

PVST doit être activé. Pour plus d'informations, consultez la section [Configurez les paramètres STP et affichez l'état STP](#), à la page 378.

Pour afficher les statistiques PVST :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > STP > Avancé > statistiques PVST**.

La page statistiques PVST s'affiche.

6. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

Si PVST est activé, le tableau suivant décrit les champs en lecture seule de la page.

Table 78 : Informations statistiques PVST

Champ	Description
Fast Backbone	
Transitions via Fast Backbone	Le nombre de transitions de backbone rapides
BPDU inférieures reçues	Nombre d'unités de données de protocole de pont inférieur (BPDU) reçues
Demandes RLQ PDU reçues	Nombre d'unités de données de protocole (PDU) de requête de liaison racine (RLQ) reçues
Réception des PDU de réponse RLQ	Nombre de PDU de réponse RLQ reçues
RLQ demande PDU envoyées	Nombre de PDU de requête RLQ transmises
Réponses RLQ PDU envoyées	Nombre de PDU de réponse RLQ transmises
Liaison montante rapide	
Transitions montantes rapides	Nombre de transitions montantes rapides
Adresses de multidiffusion proxy transmises	Nombre d'adresses de multidiffusion proxy transmises
Nom	Nom du VLAN sur lequel PVST est activé
Liste des interfaces	Interfaces qui transmettent le trafic pour le VLAN, sous forme de trames marquées ou non marquées

Base de données de transfert multidiffusion

Le trafic IP multicast est le trafic destiné à un groupe d'hôtes. Les groupes d'hôtes sont identifiés par des adresses IP de classe d, comprises entre 224.0.0.0 et 239.255.255.255.

Affiche les entrées dans la base de données de transfert multidiffusion

La base de données de transfert de multidiffusion (MFDB) contient les informations d'appartenance de port pour toutes les entrées d'adresse de multidiffusion actives. La clé d'une entrée consiste en une combinaison d'un ID VLAN et d'une adresse MAC. Les entrées peuvent contenir des données pour plusieurs protocoles.

Pour afficher les entrées dans la base de données de transfert multidiffusion :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > Multicast > MFDB > table MFDB**.

La page MFDB table s'affiche.

6. Pour rechercher une entrée, dans le champ **Rechercher par adresse MAC**, entrez une adresse MAC, puis cliquez sur le bouton **aller**.

Si l'adresse existe, cette entrée s'affiche. Une correspondance exacte est requise.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 79 : Informations MFDB

Champ	Description
Adresse MAC	Adresse MAC multicast pour laquelle vous avez demandé des données.
Identifiant VLAN	ID VLAN auquel l'adresse MAC de multidiffusion est associée.
Composante	Composant responsable de cette entrée dans la MFDB. Le composant peut être igmp snooping, GMRP, filtrage statique ou surveillance MLD.
Type	Type de l'entrée. Les entrées statiques sont celles que vous configurez. Les entrées dynamiques sont ajoutées à la table à la suite d'un processus ou d'un protocole d'apprentissage.
Description	Description de cette entrée de table multicast. La description peut être configurée pour la gestion, configurée pour le réseau ou assistée par le réseau.
Interfaces de transfert	Liste de transfert dérivée de la combinaison de toutes les interfaces de transfert et de la suppression des interfaces répertoriées comme interfaces de filtrage statique.

Supprimez les entrées igmp snooping de la base de données de transfert multidiffusion

Vous pouvez supprimer les entrées igmp snooping de la base de données de transfert multidiffusion.

Pour supprimer les entrées igmp snooping de la base de données de transfert multidiffusion :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **commutation > Multicast > MFDB > table MFDB** .
La page MFDB table s'affiche.
6. Cliquez sur le bouton **Clear** (Effacer).
Les paramètres sont enregistrés.
7. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimez toutes les entrées MAC multicast connues de la base de données de transfert multicast

Vous pouvez supprimer toutes les entrées MAC multicast connues de la base de données de transfert multicast.

Pour supprimer toutes les entrées MAC multicast connues de la base de données de transfert multicast :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > Multicast > MFDB > table MFDB**.

La page MFDB table s'affiche.

6. Cochez la case **Réinitialiser les entrées MAC de multidiffusion connues**.

Une fenêtre contextuelle de confirmation s'affiche.

7. Sélectionnez le bouton **OK**.

La fenêtre contextuelle se ferme.

8. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Afficher les statistiques de la base de données de transfert multidiffusion

Vous pouvez afficher les statistiques de la base de données de transfert multidiffusion

Pour afficher les statistiques de la base de données de transfert multidiffusion :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > Multicast > MFDB > MFDB Statistics**.

Le tableau statistiques MFDB s'affiche.

6. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

Le tableau suivant décrit les champs en lecture seule de la page.

Table 80 : Informations statistiques MFDB

Champ	Description
Nombre max. D'entrées de table MFDB	Nombre maximal d'entrées que la table de la base de données de transfert multidiffusion peut contenir.
Le plus grand nombre d'entrées MFDB depuis la dernière réinitialisation	Le plus grand nombre d'entrées présentes dans la table de la base de données de transfert multidiffusion depuis la dernière réinitialisation. Cette valeur est également connue sous le nom de seuil supérieur MFDB.
Entrées actuelles	Nombre actuel d'entrées dans la table de la base de données de transfert multidiffusion.

Surveillance du protocole de gestion de groupe Internet

La surveillance IGMP (Internet Group Management Protocol) permet au commutateur de transférer intelligemment le trafic multicast. Le trafic IP de multidiffusion est destiné à un groupe d'hôtes. Les groupes d'hôtes sont identifiés par des adresses IP de classe d, comprises entre 224.0.0.0 et 239.255.255.255. En fonction des messages de demandes et rapports IGMP, le switch transfère le trafic uniquement sur les ports qui ont demandé le trafic multicast. Cette fonctionnalité empêche le switch de diffuser le trafic sur tous les ports, ce qui pourrait affecter les performances du réseau.

Un réseau Ethernet traditionnel peut être séparé en différents segments de réseau pour éviter de placer trop de périphériques sur le même support partagé. Des ponts et des commutateurs relient ces segments. Lorsqu'un paquet avec une adresse de destination de diffusion ou de multidiffusion est reçu, le commutateur transmet une copie dans chacun des segments de réseau restants conformément à la norme IEEE MAC Bridge. Finalement, le paquet est rendu accessible à tous les noeuds connectés au réseau.

Cette approche fonctionne bien pour les paquets de diffusion qui sont destinés à être vus ou traités par tous les noeuds connectés. Dans le cas des paquets multicast, cependant, cette approche pourrait conduire à une utilisation moins efficace de la bande passante du réseau, en particulier lorsque le paquet est destiné à un petit nombre de noeuds seulement. Les paquets sont inondés dans des segments de réseau où aucun noeud n'est réceptif au paquet. Bien que les noeuds subissent rarement un surdébit de traitement pour filtrer les paquets adressés à des adresses de groupe non demandées, ils ne peuvent pas transmettre de nouveaux paquets sur le support partagé pendant la période pendant laquelle le paquet de multidiffusion est inondé. Le problème du gaspillage de bande passante est encore plus grave lorsque le segment LAN n'est pas partagé, par exemple dans les liaisons full-duplex.

Permettre aux commutateurs de surveiller les paquets IGMP est un effort créatif pour résoudre ce problème. Le commutateur utilise les informations contenues dans les paquets IGMP au fur et à mesure qu'ils sont transmis sur le réseau pour déterminer quels segments reçoivent des paquets dirigés vers l'adresse de groupe.

Configurez igmp snooping automatiquement avec le mode IGMP plus

Le mode IGMP plus vous permet de configurer automatiquement igmp snooping, qui est utilisé pour créer des listes de transfert pour le trafic multicast IPv4.

Vous pouvez également configurer igmp snooping manuellement (voir [Configurez igmp snooping manuellement](#) à la page 415).

Pour configurer igmp snooping automatiquement :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > Multicast > igmp snooping > Configuration**.

L'écran IP Configuration (Configuration IP) s'affiche.

6. Sélectionnez le bouton radio **Activer** ou **désactiver** le mode IGMP plus.

S'ils sont activés, les modes igmp snooping suivants sont automatiquement activés :

- Mode Admin
- Mode Querier proxy
- Mode d'inondation de rapport
- Exclure le mode interface Mrouter
- Quittez rapidement le mode d'affectation automatique

La valeur par défaut est Activer.

S'ils sont désactivés, ces modes igmp snooping sont automatiquement désactivés.

❗ **Remarque:** Pour plus d'informations sur les autres paramètres de la page, reportez-vous à [Configurez igmp snooping manuellement](#) à la page 415 la section .

7. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.
9. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).
Le tableau suivant décrit les champs en lecture seule de la page.

Table 81 : Informations de configuration igmp snooping

Champ	Description
Nombre de trames de contrôle multicast	Nombre de trames de contrôle multicast traitées par le commutateur.
Interfaces activées pour igmp snooping	Interfaces sur lesquelles igmp snooping est activé.
Mode de fonctionnement	Indique si igmp snooping est globalement activé ou désactivé sur le commutateur.
ID VLAN activé pour IGMP Snooping	VLAN sur lesquels igmp snooping est activé.

Configurez igmp snooping manuellement

Vous pouvez configurer manuellement les paramètres de igmp snooping, qui est utilisé pour créer des listes de transfert pour le trafic multicast IPv4.

Vous pouvez également configurer igmp snooping automatiquement (voir [Configurez igmp snooping automatiquement avec le mode IGMP plus](#) à la page 413).

Pour configurer manuellement les paramètres de igmp snooping :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.
4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **commutation > Multicast > igmp snooping > Configuration**.
L'écran IP Configuration (Configuration IP) s'affiche.
6. Sélectionnez le bouton radio **Activer** ou **désactiver** le mode Admin.
Cette sélection active ou désactive le mode d'administration de igmp snooping pour le commutateur. La valeur par défaut est désactiver.
7. Sélectionnez le bouton radio valider l'en-tête IP IGMP **Activer** ou **désactiver**.
Cette sélection active ou désactive la validation d'en-tête pour toutes les versions IGMP sur le commutateur. Si cette option est activée, un en-tête IP IGMP de paquet valide l'option Router Alert, ToS et TTL. La valeur par défaut est Activer.
8. Sélectionnez le bouton radio **Activer** ou **désactiver** le mode Querier proxy.
Cette sélection active ou désactive l'interrogateur proxy IGMP pour le commutateur. Si cette option est désactivée, la requête de proxy IGMP avec l'adresse IP source 0.0.0.0 n'est pas envoyée en réponse à un paquet IGMP Leave. La valeur par défaut est Activer.
9. Sélectionnez le bouton radio **Activer** ou **désactiver** le mode d'inondation du rapport.
Cette sélection active ou désactive le mode d'inondation du rapport sur le commutateur. Si cette option est activée, les PDU IGMP Join/Leave que le commutateur reçoit d'un hôte sur un port en aval sont transmises à tous les autres ports du VLAN associé. La valeur par défaut est Activer.
10. Sélectionnez le bouton radio exclure le mode interface Mrouter **Activer** ou **désactiver**.
Cette sélection spécifie le type d'informations qui sont transmises à l'interface du routeur multicast en amont.

Si cette option est activée, le commutateur transfère les PDU IGMP Join/Leave reçues par informatique sur un port en aval vers une interface mrouter en amont. En outre, le commutateur transmet un flux de données multidiffusion à une interface mrouter amont uniquement si ce port a déjà reçu un message d'appartenance IGMPv1 ou IGMPv2. Le commutateur supprime les flux de multidiffusion inconnus. La valeur par défaut est Activer.

Si cette option est désactivée, le commutateur transfère les PDU IGMP Join/Leave, les flux de multidiffusion connus et les flux de multidiffusion inconnus vers l'interface mrouter en amont.

11. Sélectionnez le bouton radio **Activer** ou **désactiver** le mode d'affectation automatique de congé rapide.

Cette sélection active ou désactive l'affectation automatique de messages FAST-Leave à tous les ports et LAG du commutateur. La valeur par défaut est Activer.

❗ Remarque: Pour plus d'informations sur le mode IGMP plus, reportez-vous à Configurez igmp snooping automatiquement avec le mode IGMP plus à la page 413 la section .

12. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

13. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

14. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

Le tableau suivant décrit les champs en lecture seule de la page.

Table 82 : Informations de configuration igmp snooping

Champ	Description
Nombre de trames de contrôle multicast	Nombre de trames de contrôle multicast traitées par le commutateur.
Interfaces activées pour igmp snooping	Interfaces sur lesquelles igmp snooping est activé.
Mode de fonctionnement	Indique si igmp snooping est globalement activé ou désactivé sur le commutateur.
ID VLAN activé pour IGMP Snooping	VLAN sur lesquels igmp snooping est activé.

Configurez les paramètres igmp snooping pour les interfaces

Vous pouvez configurer les paramètres igmp snooping pour les interfaces.

Pour configurer les paramètres igmp snooping des interfaces :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > Multicast > igmp snooping > Configuration de l'interface**.

La page Configuration de l'interface s'affiche.

6. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :

- **1 ou ID d'unité pour un commutateur empilé :**

- 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
 - **ID d'unité pour un commutateur empilé** : Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
 - LAG Seuls les LAG sont affichés.
 - **Tous**: Les interfaces physiques et les LAG sont affichés, ou pour une pile de commutateurs, les interfaces physiques de tous les commutateurs de la pile et les LAG sont affichés.
7. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :
- Pour afficher ou effacer les statistiques d'une seule interface, cochez la case associée à l'interface ou saisissez le numéro de l'interface dans le champ **aller à l'interface** et cliquez sur le bouton **aller**.
 - Pour configurer plusieurs interfaces avec les mêmes paramètres, cochez la case associée à chaque interface.
 - Pour configurer toutes les interfaces avec les mêmes paramètres, cochez la case dans la ligne d'en-tête.
8. Dans le menu **mode Admin**, sélectionnez **désactiver** ou **Activer**.
Cette sélection active ou désactive le mode d'administration de igmp snooping pour l'interface. La valeur par défaut est désactiver.
9. Dans le champ **intervalle d'appartenance**, spécifiez la période pendant laquelle le commutateur attend un rapport de groupe avant que informatique ne supprime l'interface en tant que membre du groupe.
Saisissez une valeur comprise entre 1 et 3600. La valeur par défaut est de 600 secondes.
10. Dans le champ **temps de réponse maximal**, spécifiez la période pendant laquelle le commutateur attend après que informatique ait envoyé une requête sur une interface car informatique n'a pas reçu de rapport d'un groupe sur cette interface.
Saisissez une valeur supérieure ou égale à 1 mais inférieure à la valeur du champ intervalle d'adhésion. La valeur par défaut est de 120 secondes.
11. Dans le champ **expiration Time**, spécifiez la période pendant laquelle le commutateur attend de recevoir une requête sur l'interface avant que informatique ne supprime l'interface de la liste des interfaces avec des routeurs multidiffusion connectés.
Entrez une valeur comprise entre 0 et 3600. La valeur par défaut est de 300 secondes. Si vous entrez 0, vous configurez un délai infini (pas d'expiration).
12. Dans le menu **départ rapide**, sélectionnez pour activer ou désactiver le mode départ rapide igmp snooping pour l'interface. Cette sélection active ou désactive l'affectation

automatique de messages de départ rapide pour l'interface. La valeur par défaut est désactiver.

Le champ mode de fonctionnement de départ rapide indique l'état de l'interface.

13. Dans le menu **Proxy Querier**, sélectionnez pour activer ou désactiver le serveur proxy pour l'interface.

Si cette option est désactivée, la requête de proxy IGMP avec l'adresse IP source 0.0.0.0 n'est pas envoyée en réponse à un paquet IGMP Leave. La valeur par défaut est Activer.

14. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

15. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez igmp snooping pour les VLAN automatiquement avec le mode IGMP plus

Le mode IGMP plus permet à NETGEAR IGMP plusTM de configurer automatiquement igmp snooping pour les VLAN et de créer des listes de transfert pour le trafic multicast.

Vous pouvez également configurer igmp snooping pour les VLAN manuellement (voir [Configurez igmp snooping manuellement](#) à la page 415).

Pour configurer igmp snooping pour VLAN automatiquement :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > Multicast > igmp snooping > Configuration igmp snooping VLAN**.

La page de configuration igmp snooping VLAN s'affiche.

6. Cochez la case en regard de l'ID VLAN.
7. Dans le menu **IGMP plus mode** à droite de la page, sélectionnez pour activer ou désactiver le mode IGMP plus sur le VLAN.

S'ils sont activés, les modes igmp snooping suivants sont automatiquement activés pour le VLAN et les événements suivants se produisent :

- Mode Admin
- Départ rapide
- Proxy Querier
- Mode d'inondation de rapport
- Exclure le mode interface Mrouter
- Installe les adresses MAC multicast réservées dans le système.

S'ils sont désactivés, ces modes igmp snooping sont automatiquement désactivés pour le VLAN.

❗ Remarque: Pour plus d'informations sur les autres paramètres de la page, reportez-vous à la section [Configurez manuellement igmp snooping pour les VLAN](#) à la page 422.

8. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez manuellement igmp snooping pour les VLAN

Vous pouvez configurer manuellement les paramètres de igmp snooping for VLAN, qui est utilisé pour créer des listes de transfert pour le trafic multicast.

Vous pouvez également configurer igmp snooping pour LES VLAN automatiquement (voir [Configurez igmp snooping pour les VLAN automatiquement avec le mode IGMP plus](#) à la page 420).

Pour configurer manuellement les paramètres de igmp snooping pour un VLAN :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > Multicast > igmp snooping > Configuration igmp snooping VLAN**.

La page de configuration igmp snooping VLAN s'affiche.

6. Cochez la case en regard de l'ID VLAN.

7. Dans le menu **mode Admin**, sélectionnez pour activer ou désactiver igmp snooping pour le VLAN.

La valeur par défaut est désactiver.

8. Dans le menu **départ rapide**, sélectionnez pour activer ou désactiver le mode départ rapide igmp snooping pour le VLAN.

Cette sélection active ou désactive l'affectation automatique de messages en attente rapide pour tous les membres du VLAN. La valeur par défaut est Activer.

9. Dans le champ **intervalle d'appartenance**, saisissez la période de l'intervalle d'appartenance au groupe de igmp snooping pour le VLAN.

La période doit correspondre à la valeur du champ temps de réponse maximum plus une valeur comprise entre 1 et 3600 secondes. La valeur par défaut est de 600 secondes.

10. Dans le champ **temps de réponse maximal**, entrez la période pour le temps de réponse maximal de igmp snooping pour le VLAN.

La plage doit être comprise entre 1 et la valeur du champ intervalle d'appartenance au groupe moins 1. La valeur du champ temps de réponse maximum doit être supérieure à celle du champ intervalle d'appartenance au groupe. La valeur par défaut est de 120 secondes.

11. Dans le champ **heure d'expiration du routeur de multidiffusion**, entrez la période d'expiration du routeur de multidiffusion de igmp snooping pour le VLAN.

La plage doit être comprise entre 0 et 3600 secondes. La valeur par défaut est de 300 secondes.

12. Dans le menu **suppression des rapports**, sélectionnez pour activer ou désactiver le mode de suppression des rapports igmp snooping pour le VLAN.

Ce mode permet la suppression des rapports IGMP envoyés par les hôtes multidiffusion. Pour ce faire, le commutateur crée une table d'appartenance de couche 3 et envoie uniquement les rapports essentiels aux routeurs IGMP qui doivent recevoir le trafic de multidiffusion. En conséquence, le trafic de rapport de multidiffusion envoyé aux routeurs IGMP est réduit. La valeur par défaut est désactiver.

13. Dans le menu **Querier proxy**, sélectionnez pour activer ou désactiver le **Querier** proxy pour VLAN.

Si cette option est désactivée, la requête de proxy IGMP avec l'adresse IP source 0.0.0.0 n'est pas envoyée en réponse à un paquet IGMP Leave. La valeur par défaut est Activer.

14. Dans le menu **mode d'inondation du rapport**, sélectionnez pour activer ou désactiver le mode d'inondation du rapport sur le VLAN.

Si cette option est activée, les PDU IGMP Join/Leave que le VLAN reçoit d'un hôte sur un port en aval sont transmises à tous les autres ports du VLAN. La valeur par défaut est Activer.

15. Dans le menu **exclure le mode interface Mrouter**, sélectionnez pour activer ou désactiver l'option exclure le mode interface Mrouter.

Cette sélection spécifie le type d'informations qui sont transmises à l'interface du routeur multicast en amont :

- Activer. Le VLAN transfère les PDU IGMP Join/Leave reçues par informatique sur un port en aval vers une interface mrouter en amont. En outre, le VLAN transmet un flux de données multidiffusion à une interface de routeur mobile amont uniquement si ce port a déjà reçu un message d'appartenance IGMPv1 ou IGMPv2. VLAN supprime les flux de multidiffusion inconnus. La valeur par défaut est Activer.
- Désactiver : Le VLAN transmet les PDU IGMP Join/Leave, les flux de multidiffusion connus et les flux de multidiffusion inconnus à l'interface mrouter en amont.

❗ Remarque: Pour plus d'informations sur le mode IGMP plus pour les VLAN, reportez-vous à la section [Configurez igmp snooping pour les VLAN automatiquement avec le mode IGMP plus](#) à la page 420.

16. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

17. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez une interface de routeur multidiffusion IGMP

Vous pouvez configurer une interface comme interface désignée à laquelle un routeur multicast est connecté. Tous les paquets IGMP surveillés par le commutateur sont transmis au routeur multicast accessible depuis cette interface. Nous appelons cette interface le routeur multicast.

Dans la plupart des cas, cette configuration n'est pas requise car le commutateur détecte automatiquement un routeur multicast et transfère les paquets IGMP en conséquence. Cette configuration peut être nécessaire dans un réseau complexe si vous voulez vous assurer que le routeur multicast reçoit toujours les paquets IGMP du commutateur.

Pour configurer une interface de routeur multicast :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > Multicast > igmp snooping > Configuration du routeur multicast**.

La page Configuration du routeur multidiffusion s'affiche.

6. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :

- **1 ou ID d'unité pour un commutateur empilé :**
 - 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
 - **ID d'unité pour un commutateur empilé :** Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
- **LAG** Seuls les LAG sont affichés.
- **Tous:** Les interfaces physiques et les LAG sont affichés, ou pour une pile de commutateurs, les interfaces physiques de tous les commutateurs de la pile et les LAG sont affichés.

7. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :

- Pour afficher ou effacer les statistiques d'une seule interface, cochez la case associée à l'interface ou saisissez le numéro de l'interface dans le champ **aller à l'interface** et cliquez sur le bouton **aller**.
 - Pour configurer plusieurs interfaces avec les mêmes paramètres, cochez la case associée à chaque interface.
 - Pour configurer toutes les interfaces avec les mêmes paramètres, cochez la case dans la ligne d'en-tête.
8. Dans le menu **Multicast Router**, sélectionnez pour activer ou désactiver l'option **Multicast Router**.
 9. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
 10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez un routeur de multidiffusion IGMP VLAN .

Vous pouvez configurer un VLAN spécifique pour une interface spécifique afin de transférer les paquets IGMP surveillés au routeur de multidiffusion connecté à l'interface.

Dans la plupart des cas, cette configuration n'est pas requise car le commutateur détecte automatiquement un routeur multicast et transfère les paquets IGMP en conséquence. Cette configuration peut être nécessaire dans un réseau complexe si vous voulez vous assurer que le routeur multicast reçoit toujours les paquets IGMP du commutateur.

Pour configurer un routeur multicast VLAN :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > Multicast > igmp snooping > Configuration VLAN du routeur multicast**.

La page Configuration VLAN du routeur multidiffusion s'affiche.

6. Dans le menu **interface**, sélectionnez l'interface.
7. Dans le champ **VLAN ID**, entrez l'ID VLAN.
8. Dans le menu **routeur multidiffusion**, sélectionnez **Activer** ou **désactiver** pour spécifier si le VLAN est un routeur multidiffusion VLAN.
9. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Présentation de l'interrogeur igmp snooping.

igmp snooping exige qu'un commutateur central ou un routeur dans un VLAN de routage interroge périodiquement tous les périphériques finaux sur le réseau pour annoncer leurs adhésions de multidiffusion. Ce périphérique central est le questeur IGMP. Les réponses aux requêtes IGMP, appelées rapports IGMP, tiennent un commutateur à jour avec l'appartenance au groupe multidiffusion actuel port par port et profil réseau. Si le commutateur ne reçoit pas les informations d'appartenance mises à jour en temps opportun, il arrête de transférer le trafic de multidiffusion vers le port où se trouve le périphérique final.

Vous pouvez configurer et afficher des informations pour les requêtes igmp snooping sur le réseau et, séparément, sur les VLAN.

Configurez les paramètres globaux du questeur igmp snooping

Vous pouvez configurer les paramètres globaux d'un interrogateur igmp snooping sur le commutateur.

Pour configurer les paramètres globaux d'un interrogateur igmp snooping :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > Multicast > igmp snooping > Configuration du Querier**.

La page Configuration du Querier s'affiche.

6. Sélectionnez le bouton radio **Activer** ou **désactiver** le mode administrateur Querier pour spécifier si igmp snooping est activé pour le commutateur.

La valeur par défaut est désactiver.

7. Dans le champ **adresse IP de l'interrogateur de surveillance**, spécifiez l'adresse IP de l'interrogateur de surveillance qui doit être utilisée comme adresse source dans les requêtes IGMP périodiques.
Cette adresse est utilisée lorsqu'aucune adresse n'est configurée sur le VLAN sur lequel les requêtes sont envoyées.
8. Dans le champ **version IGMP**, spécifiez la version du protocole IGMP utilisée dans les requêtes IGMP périodiques.
La version peut être 1 à 2. Le numéro par défaut est 2.
9. Dans le champ **intervalle de requête (secondes)**, spécifiez la période en secondes entre les requêtes périodiques envoyées par le demandeur espionneur.
La plage est de 1 à 1800 secondes. La valeur par défaut est de 60 secondes.
10. Dans le champ **intervalle d'expiration du interrogateur (secondes)**, spécifiez la période en secondes après laquelle les dernières informations du interrogateur sont supprimées.
La plage est de 60 à 300 secondes. La valeur par défaut est de 180 secondes.
11. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
La page affiche les ID VLAN activés pour le Query igmp snooping.
12. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurer un interrogateur igmp snooping pour un VLAN .

Vous pouvez configurer un interrogateur IGMP pour une utilisation avec un VLAN sur le réseau.

Configurer un interrogateur igmp snooping pour un VLAN .

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > Multicast > igmp snooping > Configuration du Querier VLAN**.

La page Configuration du Querier VLAN s'affiche.

6. Spécifiez une nouvelle VLAN ou modifiez une VLAN existante :

- **Spécifiez un nouveau VLAN** : Dans le champ **VLAN ID**, entrez l'ID d'un nouveau VLAN.
- **Modifier un VLAN existant** : Cochez la case correspondant à un VLAN existant.

7. Dans le menu **Querier Election participe mode**, sélectionnez pour activer ou désactiver le mode **Querier Election participe** :

- **Désactivé**. Si le commutateur détecte un autre interrogateur de la même version dans le VLAN, l'interrogateur de surveillance passe à l'état non interrogateur.
- **Sous tension** L'interrogateur espionneur participe à l'élection de l'interrogateur, dans laquelle l'adresse IP portant le numéro le plus bas fonctionne comme l'interrogateur dans cette VLAN. L'autre interrogateur passe à l'état non interrogateur.

Par défaut, le mode de participation aux élections du demandeur est activé pour VLAN 1.

8. Dans le champ **adresse VLAN du serveur de surveillance**, spécifiez l'adresse IP à utiliser comme adresse IP source dans les requêtes IGMP périodiques envoyées sur VLAN.
9. Ajoutez le nouveau VLAN ou enregistrez les paramètres du VLAN existant :
 - **Ajouter le nouveau VLAN** : Cliquez sur le bouton **Add** (Ajouter).

L'VLAN est ajouté.

- **Enregistrez les paramètres du VLAN existant** : Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 83 : Informations de configuration du Querier VLAN

Champ	Description
État opérationnel	L'état opérationnel de l'interrogateur igmp snooping sur un VLAN : • Querier : Le commutateur Snooping est l'interrogateur dans le VLAN. Le commutateur de surveillance envoie des requêtes périodiques avec un intervalle de temps égal à l'intervalle de requête configuré de l'interrogateur. Si le commutateur Snooping trouve un meilleur interrogateur dans le VLAN, informatique passe en mode non interrogateur. • Non-Querier : Le commutateur Snooping est en mode non-querier dans le VLAN. Si le temporisateur de l'intervalle d'expiration de l'interrogateur expire, le commutateur de surveillance passe en mode interrogateur. • Désactivé : L'interrogateur de surveillance n'est pas opérationnel sur VLAN. L'interrogateur de surveillance passe en mode désactivé lorsque igmp snooping n'est pas opérationnel sur VLAN ou lorsque l'adresse de l'interrogateur n'est pas configurée ou lorsque l'adresse de gestion réseau n'est pas configurée.
Version opérationnelle	Version opérationnelle du protocole IGMP du demandeur.
Adresse du dernier Querier	Adresse IP du dernier interrogateur à partir duquel une requête a été détectée sur VLAN.
Dernière version du Querier	Version du protocole IGMP du dernier interrogateur à partir duquel une requête a été surveillée sur VLAN.
Temps de réponse maximal opérationnel	Le temps de réponse maximal à utiliser dans les requêtes envoyées par le demandeur de surveillance.

Supprimez les paramètres de requête igmp snooping pour un VLAN

Vous pouvez supprimer les paramètres de requête igmp snooping pour un VLAN.

Pour supprimer les paramètres de requête igmp snooping pour un VLAN :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > Multicast > igmp snooping > Configuration du Querier VLAN**.

La page Configuration du Querier VLAN s'affiche.

6. Sélectionnez le VLAN pour lequel vous souhaitez supprimer les paramètres du queseur igmp snooping.

7. Cliquez sur le bouton **Supprimer**.

Les paramètres sont enregistrés. (Le VLAN lui-même n'est pas supprimé.)

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Affiche l'état du demandeur igmp snooping

Vous pouvez afficher l'état du demandeur igmp snooping pour une interface ou un VLAN.

Pour afficher l'état du demandeur igmp snooping :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > Multicast > igmp snooping Querier > table de groupes igmp snooping** .

La page Tableau des groupes igmp snooping s'affiche.

6. Pour afficher les informations d'un VLAN ou d'une interface spécifique, procédez comme suit :

- a. Dans le menu **Rechercher**, sélectionnez VLAN ID ou interface.
- b. Dans le champ, saisissez l'ID VLAN ou le numéro d'interface.
- c. Cliquez sur le bouton **GO** (Enregistrer).

7. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

Le tableau suivant décrit les champs en lecture seule de la page.

Table 84 : Informations sur le groupe igmp snooping

Champ	Description
Identifiant VLAN	ID du VLAN sur lequel l'hôte envoie des demandes de jointure de membre IGMP.
S'abonner	Adresse IP et adresse MAC de l'hôte qui envoie les demandes de jointure de membre IGMP.
Groupe MC	Adresse IP et adresse MAC de multidiffusion auxquelles l'abonné est enregistré.
Interface	L'interface sur laquelle le membre IGMP joint nous demande détecté.
Type	Version du protocole IGMP.
Délai d'attente (s)	Heure d'expiration de la mise à jour la plus récente pour cet hôte.

Surveillance de la découverte de l'écouteur multicast

Dans les réseaux IPv6, la surveillance MLD (Multicast Listener Discovery) remplit une fonction similaire à IGMP dans les réseaux IPv4. Avec MLD Snooping, les données de multidiffusion IPv6 sont transmises de manière sélective aux ports configurés pour recevoir les données, au lieu d'être inondées à tous les ports d'un VLAN. Les ports sont déterminés par la surveillance des paquets de contrôle multicast IPv6.

Un écouteur multicast est un périphérique configuré pour recevoir des paquets multicast IPv6. MLD est utilisé par les routeurs multicast IPv6 pour découvrir la présence d'auditeurs multicast sur ses liens directement attachés et pour découvrir quels paquets multicast sont d'intérêt pour les périphériques voisins.

Le protocole MLD est dérivé de IGMP. MLD version 1 (MLDv1) est équivalent à IGMPv2, et MLD version 2 (MLDv2) est équivalent à IGMPv3. MLD est un sous-protocole du protocole ICMPv6 (Internet Control message Protocol version 6), et les messages MLD sont un sous-ensemble de messages ICMPv6, identifiés dans les paquets IPv6 par une valeur d'en-tête suivant précédente de 58.

Configurez la surveillance MLD automatiquement avec le mode MLD plus

Le mode MLD plus vous permet de configurer automatiquement la surveillance MLD, qui est utilisée pour créer des listes de transfert pour le trafic multicast IPv6.

Vous pouvez également configurer manuellement la surveillance MLD (voir [Configurez manuellement la surveillance MLD](#) à la page 436).

Pour configurer automatiquement la surveillance MLD :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > Multicast > MLD Snooping > Configuration**.

L'écran IP Configuration (Configuration IP) s'affiche.

6. Sélectionnez le bouton radio **Activer** ou **désactiver** le mode MLD plus.

S'ils sont activés, les modes de surveillance MLD suivants sont automatiquement activés :

- Mode Admin MLD Snooping
- Exclure le mode interface Mrouter

La valeur par défaut est Activer.

S'ils sont désactivés, ces modes de surveillance MLD sont automatiquement désactivés.

❗ Remarque: Pour plus d'informations sur les autres paramètres de la page, reportez-vous à [Configurez manuellement la surveillance MLD](#) à la page 436 la section .

7. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.
9. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).
Le tableau suivant décrit les champs en lecture seule de la page.

Table 85 : Informations de configuration de surveillance MLD

Champ	Définition
Nombre de trames de contrôle multicast	Nombre de trames de contrôle multicast traitées.
Interfaces activées pour MLD Snooping	Interface sur laquelle MLD Snooping est activé administrativement. La surveillance MLD doit être activée globalement et sur une interface pour que l'interface puisse surveiller les paquets MLD afin de déterminer quels segments doivent recevoir des paquets multicast dirigés vers l'adresse de groupe.
ID VLAN activé pour MLD Snooping	VLAN sur lequel la surveillance MLD est activée administrativement.

Configurez manuellement la surveillance MLD

Vous pouvez configurer manuellement les paramètres de la surveillance MLD, qui est utilisée pour créer des listes de transfert pour le trafic multicast IPv6.

Vous pouvez également configurer la surveillance MLD automatiquement (voir [Configurez la surveillance MLD automatiquement avec le mode MLD plus](#) à la page 434).

Pour configurer manuellement les paramètres de surveillance MLD :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > Multicast > MLD Snooping > Configuration**.

L'écran IP Configuration (Configuration IP) s'affiche.

6. Sélectionnez le bouton radio **Activer** ou **désactiver** le mode d'administration MLD Snooping pour spécifier le mode d'administration de MLD Snooping pour le commutateur. La valeur par défaut est désactiver.

7. Sélectionnez le bouton radio **Activer** ou **désactiver** le mode Querier proxy.

Ceci active ou désactive un interrogateur proxy MLD sur le système. Si informatique est désactivé, une requête proxy MLD avec IP source 0 : :0 n'est pas envoyée en réponse à un paquet MLD Leave. Si informatique est activé, les requêtes proxy MLD sont envoyées. La valeur par défaut est Activer.

8. Sélectionnez le bouton radio exclure le mode interface Mrouter **Activer** ou **désactiver**.

Cette sélection spécifie le type d'informations qui sont transmises à l'interface du routeur multicast en amont.

Si activé, le commutateur bloque toutes les données multicast inconnues via le port mrouter, que le port soit configuré dynamiquement ou statiquement. Seules les PDU MLD sont autorisées à passer par le port mrouter vers l'interface du routeur en amont.

La valeur par défaut est Activer. Si cette option est désactivée, le commutateur transmet à la fois les données de multidiffusion inconnues et les PDU MLD à l'interface du routeur de multidiffusion en amont.

❗ Remarque: Pour plus d'informations sur le mode MLD plus, reportez-vous à la section [Configurez la surveillance MLD automatiquement avec le mode MLD plus](#) à la page 434.

9. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.
11. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).
Le tableau suivant décrit les champs en lecture seule de la page.

Table 86 : Informations de configuration de surveillance MLD

Champ	Définition
Nombre de trames de contrôle multicast	Nombre de trames de contrôle multicast traitées.
Interfaces activées pour MLD Snooping	Interface sur laquelle MLD Snooping est activé administrativement. La surveillance MLD doit être activée globalement et sur une interface pour que l'interface puisse surveiller les paquets MLD afin de déterminer quels segments doivent recevoir des paquets multicast dirigés vers l'adresse de groupe.
ID VLAN activé pour MLD Snooping	VLAN sur lequel la surveillance MLD est activée administrativement.

Configurez les paramètres de surveillance MLD pour les interfaces

Vous pouvez configurer les paramètres de surveillance MLD pour les interfaces.

Pour configurer les paramètres de surveillance MLD pour les interfaces :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > Multicast > MLD Snooping > interface Configuration**.

La page Configuration de l'interface s'affiche.

6. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :

- **1 ou ID d'unité pour un commutateur empilé :**
 - 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
 - **ID d'unité pour un commutateur empilé :** Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
- **LAG** Seuls les LAG sont affichés.
- **Tous:** Les interfaces physiques et les LAG sont affichés, ou pour une pile de commutateurs, les interfaces physiques de tous les commutateurs de la pile et les LAG sont affichés.

7. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :

- Pour afficher ou effacer les statistiques d'une seule interface, cochez la case associée à l'interface ou saisissez le numéro de l'interface dans le champ **aller à l'interface** et cliquez sur le bouton **aller**.
- Pour configurer plusieurs interfaces avec les mêmes paramètres, cochez la case associée à chaque interface.
- Pour configurer toutes les interfaces avec les mêmes paramètres, cochez la case dans la ligne d'en-tête.

8. Dans le menu **mode Admin**, sélectionnez pour activer ou désactiver la surveillance MLD pour l'interface.

La valeur par défaut est désactiver.

9. Dans le champ **intervalle d'appartenance**, spécifiez le temps pendant lequel le commutateur doit attendre un rapport pour un groupe particulier sur une interface particulière avant que informatique supprime cette interface du groupe.
La plage est de 2 à 3600 secondes. La valeur configurée doit être supérieure au temps de réponse maximal. La valeur par défaut est de 260 secondes.
10. Dans le champ **temps de réponse maximal**, spécifiez le temps d'attente du commutateur après l'envoi d'une requête sur une interface car informatique n'a pas reçu de rapport pour un groupe particulier sur cette interface.
Entrez une valeur supérieure ou égale à 1 et inférieure à l'intervalle d'adhésion en secondes. La valeur par défaut est 10 secondes. La valeur configurée doit être inférieure à l'intervalle d'adhésion.
11. Dans le champ **expiration Time**, spécifiez le délai pendant lequel le commutateur doit attendre pour recevoir une requête sur une interface avant de supprimer l'interface de la liste des interfaces avec des routeurs multidiffusion connectés.
Saisissez une valeur comprise entre 0 et 3600. La valeur par défaut est de 300 secondes. Une valeur de zéro indique un délai d'expiration infini, c'est-à-dire aucune expiration.
12. Dans le menu **quitter rapidement**, sélectionnez **Activer** ou **désactiver** pour activer ou désactiver quitter rapidement sur l'interface.
Si Fast Leave est activé, l'interface peut être immédiatement supprimée de la table de transfert de couche 2 lorsque le commutateur reçoit un message MLD Leave pour un groupe de multidiffusion sans envoyer au préalable des requêtes générales basées sur MAC. La valeur par défaut est désactiver.
13. Dans le menu **Proxy Querier**, sélectionnez **Activer** ou **désactiver** pour activer ou désactiver le mode proxy **Querier** sur l'interface.
Si le mode est désactivé, une requête proxy MLD avec IP source 0 : :0 n'est pas envoyée en réponse à un paquet MLD Leave. Si le mode est activé, les requêtes proxy MLD sont envoyées. La valeur par défaut est Activer.
14. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
15. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez la surveillance MLD pour les VLAN automatiquement avec le mode MLD plus

Le mode MLD plus vous permet de configurer automatiquement la surveillance MLD pour les VLAN, qui est utilisée pour créer des listes de transfert pour le trafic multicast IPV6.

Vous pouvez également configurer manuellement la surveillance MLD pour les VLAN (voir [Configurez igmp snooping manuellement](#) à la page 415).

Pour configurer automatiquement la surveillance MLD pour les VLAN :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > Multicast > surveillance MLD > Configuration VLAN MLD**.

La page de configuration MLD VLAN s'affiche.

6. Cochez la case correspondant à l'ID VLAN pour lequel la surveillance MLD doit être activée.

7. Dans le menu **mode MLD plus**, sélectionnez pour activer ou désactiver le mode MLD plus sur le VLAN.

S'ils sont activés, les modes de surveillance MLD suivants sont automatiquement activés pour le VLAN :

- Mode Admin
- Départ rapide
- Exclure le mode interface Mrouter

S'ils sont désactivés, ces modes de surveillance MLD sont automatiquement désactivés pour le VLAN.

❗ Remarque: Pour plus d'informations sur les autres paramètres de la page, reportez-vous à la section Configurez manuellement la surveillance MLD pour les VLAN à la page 442.

8. Cliquez sur **Ajouter** pour activer la surveillance MLD sur le VLAN spécifié.

9. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez manuellement la surveillance MLD pour les VLAN

Vous pouvez configurer manuellement les paramètres de la surveillance MLD pour les VLAN, qui est utilisée pour créer des listes de transfert pour le trafic multicast IPv6.

Vous pouvez également configurer automatiquement la surveillance MLD pour les VLAN (voir Configurez la surveillance MLD pour les VLAN automatiquement avec le mode MLD plus à la page 441).

Pour configurer manuellement les paramètres de surveillance MLD pour un VLAN :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > Multicast > surveillance MLD > Configuration VLAN MLD**.

La page de configuration MLD VLAN s'affiche.

6. Spécifiez une nouvelle VLAN ou modifiez une VLAN existante :

- **Spécifiez un nouveau VLAN** : Dans le champ VLAN ID, entrez l'ID d'un nouveau VLAN.
- **Modifier un VLAN existant** : Cochez la case correspondant à un VLAN existant.

7. Dans le menu **départ rapide**, sélectionnez pour activer ou désactiver le mode départ rapide de la surveillance MLD.

8. Dans le champ **intervalle d'appartenance**, spécifiez la période pour l'intervalle d'appartenance au groupe de surveillance MLD.

La plage s'étend de la période spécifiée dans le champ **temps de réponse maximum plus 1** à 3600 secondes. La valeur par défaut est de 260 secondes.

9. Dans le champ **temps de réponse maximal**, spécifiez la période pour le temps de réponse maximal de MLD Snooping.

La plage va de 1 seconde à la période que vous spécifiez dans **intervalle d'adhésion moins 1**. La valeur par défaut est 10 secondes.

10. Dans le champ **Multicast Router expire Time**, spécifiez la période d'expiration du routeur **Multicast** Snooping pour MLD Snooping.

La plage est de 0 à 3600 secondes. La valeur par défaut est de 300 secondes.

11. Dans le menu **Proxy Querier mode**, sélectionnez pour activer ou désactiver le mode Proxy **Querier**.

Si vous sélectionnez désactiver, la requête proxy MLD avec IP source 0 : :0 n'est pas envoyée en réponse à un paquet MLD Leave. La valeur par défaut est Activer.

12. Dans le menu **exclure le mode interface Mrouter**, sélectionnez pour activer ou désactiver le mode interface mrouter.

Cette sélection spécifie le type d'informations qui sont transmises à l'interface du routeur multicast en amont.

Si elle est activée, l'interface bloque toutes les données multicast inconnues via le port mrouter, que le port soit configuré dynamiquement ou statiquement. Seules les PDU MLD sont autorisées à passer par le port mrouter vers l'interface du routeur en amont.

La valeur par défaut est Activer. Si cette option est désactivée, l'interface transfère à la fois les données de multidiffusion inconnues et les PDU MLD à l'interface du routeur de multidiffusion en amont.

❗ Remarque: Pour plus d'informations sur le mode MLD plus pour les VLAN, reportez-vous à la section [Configurez la surveillance MLD pour les VLAN automatiquement avec le mode MLD plus](#) à la page 441.

13. Ajoutez le nouveau VLAN ou enregistrez les paramètres du VLAN existant :

- **Ajouter le nouveau VLAN** : Cliquez sur le bouton **Add** (Ajouter).
L'VLAN est ajouté.
- **Enregistrez les paramètres du VLAN existant** : Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.

14. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimez les paramètres du questeur MLD Snooping pour un VLAN

Vous pouvez supprimer les paramètres de requête MLD Snooping pour un VLAN.

Pour supprimer les paramètres de l'interrogateur MLD Snooping pour un VLAN :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > Multicast > surveillance MLD > Configuration VLAN Querier**.

La page Configuration du Querier VLAN s'affiche.

6. Sélectionnez le VLAN pour lequel vous souhaitez supprimer les paramètres du queseur igmp snooping.

7. Cliquez sur le bouton **Supprimer**.

Les paramètres sont enregistrés. (Le VLAN lui-même n'est pas supprimé.)

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez une interface de routeur multicast MLD

Vous pouvez configurer une interface comme interface désignée à laquelle un routeur multicast est connecté. Tous les paquets MLD surveillés par le commutateur sont transmis

au routeur multicast accessible depuis cette interface. Nous appelons cette interface le routeur multicast.

Dans la plupart des cas, cette configuration n'est pas requise car le commutateur détecte automatiquement un routeur multicast et transmet les paquets MLD en conséquence. Cette configuration peut être nécessaire dans un réseau complexe si vous voulez vous assurer que le routeur multicast reçoit toujours les paquets MLD du commutateur.

Pour configurer une interface de routeur multicast MLD :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > Multicast > MLD Snooping > Multicast Router Configuration**.

La page Configuration du routeur multidiffusion s'affiche.

6. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :

- **1 ou ID d'unité pour un commutateur empilé :**

- 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
 - **ID d'unité pour un commutateur empilé** : Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
 - LAG Seuls les LAG sont affichés.
 - **Tous**: Les interfaces physiques et les LAG sont affichés, ou pour une pile de commutateurs, les interfaces physiques de tous les commutateurs de la pile et les LAG sont affichés.
7. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :
- Pour afficher ou effacer les statistiques d'une seule interface, cochez la case associée à l'interface ou saisissez le numéro de l'interface dans le champ **aller à l'interface** et cliquez sur le bouton **aller**.
 - Pour configurer plusieurs interfaces avec les mêmes paramètres, cochez la case associée à chaque interface.
 - Pour configurer toutes les interfaces avec les mêmes paramètres, cochez la case dans la ligne d'en-tête.
8. Dans le menu **Multicast Router**, sélectionnez pour activer ou désactiver l'option **Multicast Router**.
9. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez un routeur de multidiffusion MLD VLAN

Vous pouvez configurer un VLAN spécifique pour une interface spécifique afin de transférer les paquets MLD surveillés au routeur de multidiffusion connecté à l'interface.

Dans la plupart des cas, cette configuration n'est pas requise car le commutateur détecte automatiquement un routeur multicast et transmet les paquets MLD en conséquence. Cette configuration peut être nécessaire dans un réseau complexe si vous voulez vous assurer que le routeur multicast reçoit toujours les paquets MLD du commutateur.

Pour configurer un routeur de multicast VLAN :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > multidiffusion > surveillance MLD > Configuration VLAN du routeur multidiffusion** .

La page Configuration VLAN du routeur multidiffusion s'affiche.

6. Dans le menu **interface**, sélectionnez l'interface.

7. Dans le champ **VLAN ID**, entrez l'ID VLAN.

8. Dans le menu **routeur multidiffusion**, sélectionnez **Activer** ou **désactiver** pour spécifier si le VLAN est un routeur multidiffusion VLAN.

9. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez les paramètres globaux du questeur MLD Snooping

Vous pouvez configurer les paramètres globaux d'un interrogateur MLD Snooping sur le commutateur.

Pour configurer les paramètres globaux d'un interrogateur MLD Snooping :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > Multicast > MLD Snooping > Configuration du Querier**.

La page Configuration du Querier s'affiche.

6. Sélectionnez le bouton radio mode administrateur Querier **Activer** ou **désactiver** pour spécifier si la surveillance MLD est activée pour le commutateur.

La valeur par défaut est désactiver.

7. Dans le champ **Querier Address**, spécifiez l'adresse IP du **Querier** Snooping qui doit être utilisée comme adresse source dans les requêtes MLD périodiques.

Cette adresse est utilisée lorsqu'aucune adresse n'est configurée sur le VLAN sur lequel les requêtes sont envoyées. Les formats IPv6 pris en charge sont x:x:x:x:x:x:x et x::x.

! Remarque: Le champ version MLD indique toujours la version 1 du protocole MLD. Il s'agit de la version utilisée dans les requêtes MLD périodiques.

8. Dans le champ **intervalle de requête (secondes)**, spécifiez la période en secondes entre les requêtes périodiques envoyées par le demandeur espionneur.

La plage est de 1 à 1800 secondes. La valeur par défaut est de 60 secondes.

9. Dans le champ **intervalle d'expiration du interrogateur (secondes)**, spécifiez la période en secondes après laquelle les dernières informations du interrogateur sont supprimées.

La plage est de 60 à 300 secondes. La valeur par défaut est de 60 secondes.

10. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

La page affiche les ID VLAN activés pour le demandeur de surveillance MLD.

11. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurer un interrogateur igmp snooping pour un VLAN .

Vous pouvez configurer un interrogateur MLD pour une utilisation avec un VLAN sur le réseau.

Configurer un interrogateur igmp snooping pour un VLAN .

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > multidiffusion > surveillance MLD > Configuration VLAN Querier**.

La page Configuration du Querier VLAN s'affiche.

6. Spécifiez une nouvelle VLAN ou modifiez une VLAN existante :

- **Spécifiez un nouveau VLAN** : Dans le champ VLAN ID, entrez l'ID d'un nouveau VLAN.
- **Modifier un VLAN existant** : Cochez la case correspondant à un VLAN existant.

7. Dans le menu **Querier Election participe mode**, sélectionnez pour activer ou désactiver le mode **Querier Election participe** :

- Désactiver : Si le commutateur détecte un autre interrogateur de la même version dans le VLAN, l'interrogateur de surveillance passe à l'état non interrogateur.
- Activer. L'interrogateur espionneur participe à l'élection de l'interrogateur, dans laquelle l'adresse IPv6 portant le numéro le plus bas fonctionne comme l'interrogateur dans cette VLAN. L'autre interrogateur passe à l'état non interrogateur.

8. Dans le champ **adresse VLAN du Querier**, spécifiez l'adresse IPv6 à utiliser comme adresse source dans les requêtes IGMP périodiques envoyées sur VLAN.

9. Ajoutez le nouveau VLAN ou enregistrez les paramètres du VLAN existant :

- **Ajouter le nouveau VLAN** : Cliquez sur le bouton **Add** (Ajouter).
L'VLAN est ajouté.
- **Enregistrez les paramètres du VLAN existant** : Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 87 : Informations de configuration du Querier VLAN

Champ	Description
État opérationnel	État opérationnel du questeur MLD Snooping sur un VLAN : • Querier : Le commutateur Snooping est l'interrogateur dans le VLAN. Le commutateur de surveillance envoie des requêtes périodiques avec un intervalle de temps égal à l'intervalle de requête configuré de l'interrogateur. Si le commutateur Snooping trouve un meilleur interrogateur dans le VLAN, informatique passe en mode non interrogateur. • Non-Querier : Le commutateur Snooping est en mode non interrogateur dans le VLAN. Si le temporisateur de l'intervalle d'expiration de l'interrogateur expire, le commutateur de surveillance passe en mode interrogateur. • Désactivé : L'interrogateur de surveillance n'est pas opérationnel sur VLAN. L'interrogateur de surveillance passe en mode désactivé lorsque la surveillance MLD n'est pas opérationnelle sur VLAN ou lorsque l'adresse de l'interrogateur n'est pas configurée ou que l'adresse de gestion réseau n'est pas configurée.
Version opérationnelle	Version opérationnelle du protocole MLD du demandeur
Adresse du dernier Querier	Adresse IP du dernier interrogateur à partir duquel une requête a été détectée sur VLAN
Dernière version du Querier	Version du protocole MLD du dernier interrogateur à partir duquel une requête a été surveillée sur VLAN
Temps de réponse maximal opérationnel	Le temps de réponse maximal à utiliser dans les requêtes envoyées par le demandeur de surveillance

Supprimez les paramètres du questeur MLD Snooping pour un VLAN

Vous pouvez supprimer les paramètres de requête MLD Snooping pour un VLAN.

Pour supprimer les paramètres de l'interrogateur MLD Snooping pour un VLAN :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > multidiffusion > surveillance MLD > Configuration VLAN Querier**.

La page Configuration du Querier VLAN s'affiche.

6. Sélectionnez le VLAN pour lequel vous souhaitez supprimer les paramètres du queseur igmp snooping.

7. Cliquez sur le bouton **Supprimer**.

Les paramètres sont enregistrés. (Le VLAN lui-même n'est pas supprimé.)

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Multicast VLAN Registration

IGMP et MLD Snooping aident à limiter le trafic multicast lorsque les ports membres sont dans le même VLAN. Cependant, lorsque les ports appartiennent à des VLAN différents, une copie du flux de multidiffusion est envoyée à chaque VLAN avec des ports membres dans le groupe de multidiffusion. L'enregistrement VLAN multicast élimine le besoin de dupliquer le trafic multicast lorsque les ports des membres du groupe multicast appartiennent à des VLAN différents.

Le conducteur utilise un VLAN multicast dédié pour transférer le trafic multicast sur le réseau L2. Vous ne pouvez configurer qu'un seul réseau local virtuel (VLAN) source multicast (MVLAN) sur le commutateur. Un tel MVLAN est utilisé uniquement pour certains trafics multicast, tels que le trafic provenant d'une application IPTV, afin d'éviter la duplication de flux multicast pour les clients dans différents VLAN. Les clients peuvent rejoindre ou quitter dynamiquement le MVLAN sans interférer avec leur appartenance à d'autres VLAN.

MVR, comme IGMP et MLD Snooping, permet à un commutateur de couche 2 d'écouter les messages IGMP et MLD pour en savoir plus sur l'appartenance à un groupe de multidiffusion.

Vous pouvez configurer les paramètres globaux, de groupe, d'interface et d'appartenance à un groupe.

Configurez les paramètres globaux du conducteur

Vous pouvez configurer les paramètres généraux du dossier conducteur qui s'appliquent au commutateur.

Pour configurer les paramètres globaux du dossier conducteur :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **commutation > dossier patient > basique > Configuration dossier patient**.
L'écran MVR Configuration (Configuration IP) s'affiche.
6. Dans le menu **d'exécution du dossier patient**, sélectionnez **Activer** ou **désactiver** pour spécifier si le dossier patient est activé ou désactivé globalement sur le commutateur
La valeur par défaut est désactiver.
7. Dans le champ **VLAN de multidiffusion du dossier du conducteur**, spécifiez l'VLAN sur laquelle les données de multidiffusion du dossier du conducteur sont reçues.
Tous les ports source appartiennent à ce VLAN. La plage est de 1 à 4093. La valeur par défaut 1.
8. Dans le champ **temps de réponse à la requête globale du conducteur**, définissez la période pendant laquelle le commutateur doit attendre un rapport d'appartenance à un groupe IGMP à partir d'une interface avant de supprimer l'interface en tant que membre du groupe de multidiffusion.
Cette période s'applique uniquement au retrait de l'interface du port récepteur sur le commutateur. Lorsqu'une requête IGMP est envoyée à partir d'un port de récepteur, le commutateur attend l'heure par défaut ou configurée de requête du conducteur pour un rapport d'appartenance à un groupe IGMP avant de supprimer l'interface en tant que membre du groupe de multidiffusion. La période est égale à un dixième de seconde. La plage est de 1 à 100 secondes. La valeur par défaut est de 5 dixièmes ou demi.
9. Sélectionnez le bouton radio **compatible avec** le mode du conducteur ou **dynamique** pour spécifier le mode de fonctionnement du conducteur.
Sélectionnez le bouton radio **compatible** (mode par défaut) pour bloquer les rapports d'appartenance à un groupe IGMP sur les ports source. Sélectionnez le bouton radio **dynamique** pour autoriser les rapports d'appartenance à un groupe IGMP sur les ports source.
10. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
11. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.
12. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).
Le tableau suivant décrit les champs en lecture seule de la page.

Table 88 : Informations de configuration du dossier patient conducteur

Champ	Définition
Groupes de multidiffusion max. Du dossier du conducteur	Nombre maximal de groupes de multidiffusion pris en charge par le dossier conducteur.
Groupes de multidiffusion actuels du dossier du conducteur	Nombre de groupes de dossier conducteur attribués.

Configurer un groupe de dossier conducteur

Vous pouvez configurer un groupe de dossier patient conducteur. Après avoir configuré les interfaces pour le dossier du conducteur, vous pouvez les ajouter en tant que membres du groupe du dossier du conducteur.

Pour configurer un groupe de dossier conducteur :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > conducteur > Avancé > Configuration du groupe de conducteur**.

La page Configuration du groupe du conducteur s'affiche.

6. Dans le champ **IP du groupe du conducteur**, spécifiez l'adresse IP du nouveau groupe du conducteur.
7. Dans le champ **nombre**, spécifiez le nombre de groupes de dossier patient contigus.
Ce numéro vous aide à créer plusieurs groupes de dossier patient en cliquant simplement sur le bouton **Ajouter**. Si le champ est vide, cliquer sur le bouton crée un seul nouveau groupe. Le champ est affiché comme vide pour chaque groupe particulier. La plage est de 1 à 256.
8. Cliquez sur le bouton **Add** (Ajouter).
Le groupe MVR est ajouté.
9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 89 : Informations de configuration du groupe du dossier patient conducteur

Champ	Définition
Etat	Statut du groupe de dossier conducteur spécifique.
Membres	Liste des interfaces qui participent au groupe du dossier du conducteur.

Supprimer un groupe de dossier du conducteur

Vous pouvez supprimer une règle de trafic dont vous n'avez plus besoin.

Pour supprimer un groupe de dossier patient :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > conducteur > Avancé > Configuration du groupe de conducteur**.

La page Configuration du groupe du conducteur s'affiche.

6. Cochez la case correspondant au groupe du dossier du conducteur.

7. Cliquez sur le bouton **Supprimer**.

Le groupe du dossier du conducteur est supprimé.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurer une interface du conducteur

Nous vous recommandons de configurer une interface de dossier conducteur avant d'ajouter informatique en tant que membre d'un groupe de dossier conducteur.

Pour configurer une interface du conducteur :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > conducteur > Avancé > Configuration de l'interface conducteur**.

La page Configuration de l'interface du conducteur s'affiche.

6. Si une pile est configurée, indiquez si vous souhaitez afficher les interfaces physiques d'un commutateur ou de tous les commutateurs de la pile :

- **ID d'unité pour un commutateur empilé** : Les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
Si aucune pile de commutateurs n'est configurée, la seule option est l'ID d'unité 1.
- **Tous** : Les interfaces physiques de tous les commutateurs de la pile sont affichées.
Si aucune pile de commutateurs n'est configurée, l'option tous n'a aucun effet.

7. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :

- Pour afficher ou effacer les statistiques d'une seule interface, cochez la case associée à l'interface ou saisissez le numéro de l'interface dans le champ **aller à l'interface** et cliquez sur le bouton **aller**.
- Pour configurer plusieurs interfaces avec les mêmes paramètres, cochez la case associée à chaque interface.
- Pour configurer toutes les interfaces avec les mêmes paramètres, cochez la case dans la ligne d'en-tête.

8. Dans le menu **mode Admin**, spécifiez si le dossier du conducteur est activé sur l'interface en sélectionnant **Activer** ou **désactiver**.

La valeur par défaut est désactiver.

9. Dans le menu **type**, spécifiez si l'interface est un récepteur du conducteur ou une source du conducteur en sélectionnant **récepteur** ou **source**.

Le type de port par défaut est none.

10. Dans le menu **quitter immédiatement**, spécifiez si la fonction quitter immédiatement est activée en sélectionnant **Activer** ou **désactiver**.

La valeur par défaut est désactiver.

11. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

12. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

13. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

Le champ État indique l'état de chaque interface.

Configurer les membres de l'interface d'un groupe de dossier conducteur

Vous pouvez ajouter ou supprimer des interfaces en tant que membres d'un groupe de dossier patient.

Pour configurer les membres de l'interface d'un groupe de dossier patient :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **commutation > dossier du conducteur > Avancé > appartenance au groupe du dossier du conducteur**.
La page appartenance au groupe du dossier du conducteur s'affiche.
Les ports du commutateur (unité 1) sont affichés. Si une pile est configurée, les ports de chaque commutateur empilé (unité 1, unité 2, etc.) sont affichés et vous pouvez sélectionner des ports sur différents commutateurs empilés.
6. Dans le menu **IP du groupe**, sélectionnez l'adresse IP du groupe du dossier conducteur.
7. Dans la table ports (ou, si une pile est configurée, dans une ou plusieurs tables ports), cliquez sur chaque port que vous souhaitez rendre membre du groupe du conducteur.
Un port sélectionné est indiqué par une coche.
8. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Afficher les statistiques du dossier du conducteur

Vous pouvez afficher les statistiques du dossier du conducteur pour le commutateur. Ces statistiques sont associées à IGMP.

Pour afficher les statistiques du dossier du conducteur :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > dossier patient > Avancé > statistiques dossier patient**.

La page statistiques MVR s'affiche.

6. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

Le tableau suivant décrit les champs en lecture seule de la page.

Table 90 : Informations statistiques MVR

Champ	Définition
Requête IGMP reçue	Nombre de requêtes IGMP reçues.
Rapport IGMP V1 reçu	Nombre de rapports IGMP V1 reçus.
Rapport IGMP V2 reçu	Nombre de rapports IGMP V2 reçus.
Congé IGMP reçu	Nombre de feuilles IGMP reçues.
Requête IGMP transmise	Nombre de requêtes IGMP transmises.
Rapport IGMP V1 transmis	Nombre de rapports IGMP V1 transmis.
Rapport IGMP V2 transmis	Nombre de rapports IGMP V2 transmis.
Congé IGMP transmis	Nombre de feuilles IGMP transmises.
Échecs de réception de paquets IGMP	Nombre d'échecs de réception de paquets IGMP.
Échecs de transmission de paquets IGMP	Nombre d'échecs de transmission de paquets IGMP.

Table d'adresse MAC

Vous pouvez afficher ou configurer la table d'adresses MAC. Ce tableau contient des informations sur les entrées de monodiffusion pour lesquelles le commutateur contient des informations de transfert ou de filtrage. Ces informations permettent à la fonction de pontage transparent de déterminer comment une trame entrante doit être propagée.

Affichez, recherchez ou effacez la table d'adresses MAC

Si vous effacez les entrées d'adresse MAC de la table d'adresses MAC, seules les entrées dynamiques sont supprimées.

Pour afficher, rechercher ou effacer la table d'adresses MAC :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > table d'adresses > basique > table d'adresses**.

La page table d'adresses s'affiche.

6. Utilisez le menu et le champ **Rechercher** pour rechercher une adresse MAC, un ID VLAN ou un numéro d'interface :

- **Recherche par adresse MAC** : Dans le menu **Rechercher**, sélectionnez adresse MAC, puis entrez l'adresse MAC hexadécimale de 6 octets dans des groupes de deux chiffres séparés par des deux-points, par exemple 01:23:45:67:89:ab. Cliquez ensuite sur le bouton **aller**.

Si l'adresse existe, cette entrée est affichée en tant que première entrée, suivie des adresses MAC restantes (supérieures). Une correspondance exacte est requise.

- **Rechercher un ID VLAN** : Dans le menu **Rechercher**, sélectionnez ID VLAN, puis entrez l'ID VLAN, par exemple, 100. Cliquez ensuite sur le bouton **aller**.
- **Interface de recherche** : Dans le menu **Rechercher**, sélectionnez **Port**, puis entrez l'ID d'interface en utilisant la convention de dénomination d'interface correspondante (par exemple, 0/2). Cliquez ensuite sur le bouton **aller**.

7. Pour supprimer les entrées dynamiques de la table d'adresses MAC, cliquez sur le bouton **Effacer**.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

9. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

Le tableau suivant décrit les champs en lecture seule de la page.

Table 91 : Informations sur la table d'adresses MAC

Champ	Description
Adresse MAC totale	Nombre total d'adresses MAC apprises ou configurées.
Adresse MAC	Adresse MAC de monodiffusion pour laquelle le commutateur contient des informations de transfert, de filtrage ou à la fois des informations de transfert et de filtrage. Le format est une adresse MAC de 6 octets séparée par deux-points, par exemple 01:23:45:67:89:ab.
Identifiant VLAN	ID VLAN associé à l'adresse MAC.
Port	Interface sur laquelle l'adresse a été apprise.
Etat	Statut de cette entrée : • Statique L'adresse MAC a été ajoutée par le commutateur ou un utilisateur et ne peut pas être reclassifiée. • Appris: L'adresse MAC a été apprise et est utilisée. • Administration Adresse MAC de gestion.

Définissez l'intervalle de vieillissement des adresses dynamiques.

Vous pouvez définir l'intervalle d'ancienneté des adresses pour la base de données de transfert. Il s'agit de la période de temporisation en secondes pour les informations de transfert acquises dynamiquement.

Définissez l'intervalle de vieillissement des adresses dynamiques.

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > table d'adresses > Avancé > adresses dynamiques**

.

La page adresses dynamiques s'affiche.

6. Dans le champ **délai d'expiration de l'adresse (secondes)**, spécifiez le délai d'expiration en secondes pour les informations de transfert acquises dynamiquement.

La plage est de 10 à 1000000 secondes. La valeur par défaut est de 3000 secondes.

7. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Ajoutez une adresse MAC statique à la table d'adresses MAC.

Les entrées d'adresses MAC statiques sont celles que vous ajoutez manuellement à la table d'adresses MAC pour une interface et un VLAN spécifiques.

Ajoutez une adresse MAC statique à la table d'adresses MAC.

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > table d'adresses > Avancé > adresse MAC statique**.

La page adresse MAC statique s'affiche.

6. Dans le menu **interface**, sélectionnez l'interface ou lag.

7. Dans le champ **adresse MAC statique**, entrez l'adresse MAC.
8. Dans le menu **VLAN ID**, sélectionnez l'ID VLAN qui doit être associé à l'adresse MAC.
9. Cliquez sur le bouton **Add** (Ajouter).
L'adresse MAC statique est ajoutée à la table des adresses MAC.
10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Ajoutez une adresse MAC statique à la table d'adresses MAC.

Vous pouvez supprimer une adresse MAC statique dont vous n'avez plus besoin.

Pour supprimer une adresse MAC statique de la table d'adresses MAC :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.
4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > table d'adresses > Avancé > adresse MAC statique**

La page adresse MAC statique s'affiche.

6. Dans le menu **interface**, sélectionnez l'interface ou lag.

7. Cochez la case correspondant à l'adresse MAC.

8. Cliquez sur le bouton **Supprimer**.

L'adresse MAC statique est supprimée de la table d'adresses MAC.

9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Paramètres des ports

Pour les ports physiques et les LAG sur le commutateur, vous pouvez configurer et afficher les paramètres, y compris le mode d'administration d'un port ou d'un lag (activé par défaut) et les paramètres de vitesse d'un port (détecté automatiquement par défaut), ajouter des descriptions de port, afficher des informations sur les émetteurs-récepteurs de port optionnels que vous pourriez avoir installés et configurer les paramètres de volet de liaison de port.

Configurez et affichez les paramètres du port

Vous pouvez configurer et afficher les informations relatives au port physique du commutateur. Certains paramètres qui s'appliquent aux ports physiques ne s'appliquent pas aux LAG.

❗ Remarque: Si vous modifiez la négociation automatique, la vitesse ou le mode duplex d'un port physique, le commutateur peut être inaccessible pendant un certain nombre de secondes pendant que les nouveaux paramètres prennent effet.

Pour configurer et afficher les paramètres du port :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > ports > Configuration des ports** .

La page Configuration du port s'affiche.

6. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :

- **1 ou ID d'unité pour un commutateur empilé :**
 - 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
 - **ID d'unité pour un commutateur empilé :** Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
- **LAG** Seuls les LAG sont affichés.
- **Tous:** Les interfaces physiques et les LAG sont affichés, ou pour une pile de commutateurs, les interfaces physiques de tous les commutateurs de la pile et les LAG sont affichés.

7. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :

- Pour afficher ou effacer les statistiques d'une seule interface, cochez la case associée à l'interface ou saisissez le numéro de l'interface dans le champ **aller à l'interface** et cliquez sur le bouton **aller**.
- Pour configurer plusieurs interfaces avec les mêmes paramètres, cochez la case associée à chaque interface.
- Pour configurer toutes les interfaces avec les mêmes paramètres, cochez la case dans la ligne d'en-tête.

8. Dans le menu **mode STP**, sélectionnez pour activer ou désactiver le mode d'administration du protocole Spanning Tree pour le port ou lag.
La valeur par défaut est Activer.
9. Dans le menu **mode Admin**, sélectionnez pour activer ou désactiver le mode administratif pour le port ou lag.
Pour que le port ou lag participe au réseau, vous devez sélectionner **Activer**. La valeur par défaut est Activer.
10. Dans le menu **LACP mode**, sélectionnez pour activer ou désactiver le mode d'administration Link Aggregation Control Protocol pour le port.
Le mode doit être activé pour que le port participe à l'agrégation de liens. La valeur par défaut est Activer.
11. Dans le menu négociation automatique, sélectionnez pour activer ou désactiver le mode de négociation automatique de la vitesse pour le port.
La valeur par défaut est Activer.
12. Pour modifier la vitesse du port, dans le champ **vitesse**, saisissez la vitesse prise en charge :
Pour les ports Gigabit Ethernet :
 - **Auto**. La vitesse est définie par le processus de négociation automatique. Il s'agit de l'option par défaut.
 - 1000. La vitesse est définie sur 1000 Mbits/s (Mbits/s)
 - 100. La vitesse est limitée à 100 Mbits/s.
Pour les ports Ethernet multivitesse :
 - **Auto**. La vitesse est définie par le processus de négociation automatique. Il s'agit de l'option par défaut.
 - 10G : La vitesse est définie sur 10 Gbits/s (Gbits/s)
 - 5G : La vitesse est limitée à 5 Gbits/seconde.
 - 2.5G : La vitesse est limitée à 2,5 Gbits/seconde.
 - 1000. La vitesse est limitée à 1000 Mbits/s.

Les caractères de délimitation pour définir différentes valeurs de vitesse sont une virgule (,), un point (.) et un espace (). Pour que vous puissiez définir la vitesse de négociation automatique, le mode de négociation automatique doit être **activé**.

❗ Remarque: Vous pouvez définir la vitesse des ports Ethernet. Pour les ports SFP, la vitesse est automatiquement détectée et vous ne pouvez pas la modifier.
13. Pour modifier le mode duplex du port, dans le menu **mode duplex**, sélectionnez l'une des valeurs suivantes :

- **Auto.** La vitesse est définie par le processus de négociation automatique. Il s'agit de l'option par défaut.
 - **Complet:** La transmission entre les dispositifs se fait simultanément dans les deux sens.
 - **Semi-duplex** La transmission entre les appareils se fait dans une seule direction à la fois.
14. Dans le menu **interruption de liaison**, sélectionnez pour activer ou désactiver l'option d'envoi d'interruption lorsque l'état du port ou de la liaison lag change.
- Pour les ports, la valeur par défaut est Activer. Pour les LAG, la valeur par défaut est désactiver.
15. Dans le champ **taille de trame**, spécifiez la taille de trame Ethernet maximale prise en charge par le port ou lag, y compris l'en-tête Ethernet, le CRC et la charge utile. La plage est de 1500 à 12270. Le numéro par défaut est 9198.
16. Dans le champ **délai de rebond**, spécifiez la période d'attente pour le rebond du port ou du lag.
- Spécifiez la période comme un multiple de 100 millisecondes (ms) dans la plage de 100 à 5000. La valeur par défaut est 0 seconde, ce qui signifie que l'anti-rebond est désactivé.
17. Dans le menu **contrôle de flux**, sélectionnez la configuration du contrôle de flux IEEE 802.3x pour le port :
- **Désactiver :** Si les tampons de port sont pleins, le commutateur n'envoie pas de trames pause et une perte de données peut se produire. Il s'agit de l'option par défaut.
 - **Symétrique:** Si les tampons de port sont pleins, le commutateur envoie des trames pause pour arrêter le trafic.
- Le contrôle de flux permet d'éviter la perte de données lorsque le port ne peut pas suivre le nombre de trames commutées. Avec un contrôle de flux symétrique, le commutateur peut envoyer une trame pause pour arrêter le trafic sur le port si la quantité de mémoire utilisée par les paquets sur le port dépasse un seuil préconfiguré et répond aux demandes de pause des périphériques partenaires. Le port mis en pause ne transfère pas les paquets pendant la durée spécifiée dans la trame pause. Lorsque le temps de pause des trames est écoulé ou que l'utilisation revient à un seuil bas spécifié, le commutateur permet au port de transmettre à nouveau des trames. Le commutateur honore également les trames pause entrantes en arrêtant temporairement la transmission.
- **Asymétrique:** Si les tampons de port sont pleins, le commutateur n'envoie pas de trames pause et une perte de données peut se produire. Cependant, le commutateur honore les trames de pause entrantes en arrêtant temporairement la transmission.

18. Dans le champ **intervalle de chargement**, spécifiez la période d'intervalle de chargement pour le port ou lag.

Il s'agit de la période pendant laquelle les données sont utilisées pour calculer les statistiques de charge. Entrez la période par multiples de 30 secondes, de 30 à 600. La valeur par défaut est de 300 secondes. Plus l'intervalle de charge est petit, plus le taux instantané pour les statistiques de charge est précis.

19. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

20. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 92 : Informations sur la configuration du port

Champ	Description
Type de média	Type de support pris en charge par le port.
Type de port	Pour les ports normaux, ce champ est normal. Les valeurs possibles sont les suivantes : • Miroirs Le port est un port miroir sur lequel tout le trafic est copié vers le port sonde. • Sonde : Utilisez ce port pour surveiller un port en miroir. • Membre du réseau : Le port est membre d'une jonction d'agrégation de liens. Consultez les pages lag pour plus d'informations.
État physique	La vitesse du port et le mode duplex.
Etat de liaison	Indique si le port ou la liaison lag est actif ou inactif.
IfIndex	IfIndex de l'entrée de la table d'interface associée au port ou lag.

Ajoutez des descriptions de port, lag et VLAN

Vous pouvez ajouter une description pour un port, lag et VLAN.

Pour ajouter des descriptions de port, lag et VLAN :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > ports > Description du port**.

La page Description du port s'affiche.

6. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :

- **1 ou ID d'unité pour un commutateur empilé :**
 - 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
 - **ID d'unité pour un commutateur empilé :** Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
- **LAG** Seuls les LAG sont affichés.
- **VLAN** Seuls les VLAN sont affichés.
- **Tous:** Les interfaces physiques, les LAG et les VLAN sont affichés, ou pour une pile de commutateurs, les interfaces physiques de tous les commutateurs de la pile, les LAG et les VLAN sont affichés.

7. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :

- Pour configurer une interface ou un VLAN unique, cochez la case associée à l'interface ou au VLAN, ou tapez le numéro de l'interface ou du VLAN dans le champ **aller à l'interface** et cliquez sur le bouton **aller**.
 - Pour configurer plusieurs interfaces ou VLAN avec les mêmes paramètres, cochez la case associée à chaque interface ou VLAN.
 - Pour configurer toutes les interfaces, VLAN ou les deux interfaces et VLAN avec les mêmes paramètres, cochez la case dans la ligne d'en-tête.
8. Dans le champ Nom, entrez un nom de 64 caractères maximum.
9. Cliquez sur le bouton **Apply** (Appliquer).
- Les paramètres sont enregistrés.
10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 93 : Informations sur la description du port

Champ	Description
Adresse MAC	Adresse MAC de l'interface ou de l'VLAN.
Décalage des bits de la liste des ports	Valeur de décalage de bit qui correspond à l'interface ou au VLAN lorsque le type d'objet MIB PortList est utilisé pour gérer dans SNMP.
IfIndex	Index de l'interface associé à l'interface ou au VLAN.

Affiche les informations du module émetteur-récepteur

Pour activer la fibre haut débit et l'Ethernet Gigabit, les connexions courte et longue distance sur le commutateur, les ports fibre SFP, SFP+ et SFP28 peuvent accueillir les modules émetteurs-récepteurs standard 1G SFP, 10G SFP+ et SFP28 25G. Vous pouvez afficher les informations relatives au module émetteur-récepteur pour tous les ports fibre optique du commutateur.

Pour afficher les informations sur le module émetteur-récepteur :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > ports > émetteur-récepteur de port**.

La page Port Transceiver s'affiche.

6. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

Le tableau suivant décrit les champs en lecture seule de la page.

Table 94 : Informations sur le port émetteur-récepteur

Champ	Description
Port	Port dans lequel le module émetteur-récepteur est installé.
Nom du fournisseur	Nom du fournisseur du module émetteur-récepteur.
Longueur de maillon 50 µm [m]	Longueur de liaison prise en charge pour la fibre optique de 50 µm.
Longueur de maillon 62,5 µm [m]	Longueur de liaison prise en charge pour la fibre optique de 62,5 µm.
Numéro de série	Numéro de série du module émetteur-récepteur.
Référence	Numéro de pièce du module émetteur-récepteur.
Débit binaire nominal [Mbps]	Débit de signalisation nominal pour le module émetteur-récepteur.
Révision	Révision du fournisseur du module émetteur-récepteur.
Conformité	La conformité du module émetteur-récepteur.

Table 94 : Informations sur le port émetteur-récepteur (A continué)

Champ	Description
Prises en charge	Indique si le module émetteur-récepteur inséré est réellement pris en charge (Oui ou non).
Vitesse possible détectée	Vitesse potentielle prise en charge par le module émetteur-récepteur.

Configurez les paramètres du volet de liaison du port

Vous pouvez configurer les paramètres de volet de liaison de port, qui déterminent quand un port est automatiquement placé à l'état désactivé. Vous pouvez également configurer les paramètres de récupération automatique, ce qui permet d'activer à nouveau automatiquement un port.

Pour configurer les paramètres du volet de liaison du port :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > ports > Configuration du volet de liaison**.

La page Link Flap Configuration s'affiche.

6. Sélectionnez la case d'option **Activer** ou **désactiver** le mode Admin pour activer ou désactiver le mode d'administration Link Flap.

Pour pouvoir configurer les paramètres du volet de liaison, vous devez sélectionner **Activer**. La valeur par défaut est **désactiver**.

7. Dans le champ **Max-Count**, entrez le nombre maximal de volets autorisés avant que le port ne soit placé à l'état désactivé.

Vous pouvez définir un nombre compris entre 2 et 10. Par défaut, le nombre est 5.

8. Dans le champ **durée**, entrez la période maximale en secondes pendant laquelle le nombre de volets de liaison est compté.

Si le nombre de volets de liaison sur le port est supérieur ou égal au nombre que vous entrez dans le champ **Max-Count**, le port est placé à l'état désactivé. Par défaut, la période est de 10 secondes. Vous pouvez entrer une période de 3 à 200 secondes.

9. Sélectionnez le bouton radio **Activer** ou **désactiver** le mode d'administration de récupération automatique pour activer ou désactiver le mode d'administration de récupération automatique.

Pour activer la récupération automatique, vous devez sélectionner **Activer**. Si cette option est activée, le port est automatiquement retiré de l'état désactivé une fois l'intervalle atteint. La valeur par défaut est **désactiver**.

10. Dans le champ **intervalle de récupération automatique**, entrez la période en secondes après laquelle le port est automatiquement retiré de l'état désactivé.

Vous pouvez entrer une période comprise entre 30 et 86400 secondes. La période par défaut est de 300 secondes.

11. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

La section d-Disabled ports due à Link Flap répertorie les ports qui sont à l'état désactivé.

12. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Lier les groupes d'agrégation

Les groupes d'agrégation de liens (LAG), également appelés canaux de port, vous permettent de combiner plusieurs liaisons Ethernet full-duplex en une seule liaison

logique. Les périphériques réseau traitent l'agrégation en tant que liaison unique, ce qui améliore la tolérance aux pannes et le partage de charges. Vous attribuez l'adhésion VLAN lag après avoir créé un lag. Le lag devient par défaut membre du VLAN de gestion.

Une interface lag peut être statique ou dynamique, mais pas les deux. Tous les éléments d'un LAG doivent se trouver sur le même VLAN. Une interface port-canal statique ne nécessite pas qu'un système partenaire puisse agréger ses ports membres.

Ce switch prend en charge les LAG statiques. Lorsqu'un port est ajouté en tant que membre statique à un lag, le port ne transmet ni ne reçoit de LACPDU.

Présentation de Auto-lag

Un auto-lag est un lag qui se forme automatiquement entre deux périphériques prenant en charge la fonction Auto-lag. Un lag automatique est un protocole lag dynamique de couche 2 basé sur le protocole LACP (Link Aggregation Control Protocol).

❗ Remarque: Un lag est également appelé canal de port ou EtherChannel.

Le commutateur peut détecter les liaisons physiques avec un périphérique partenaire et configurer automatiquement un lag (c'est-à-dire un auto-lag) sur les ports interconnectés et compatibles aux deux extrémités. Le commutateur peut former un auto-lag uniquement avec chaque périphérique partenaire.

La fonction Auto-lag fonctionne avec la fonction Auto-Trunk, qui doit également être prise en charge et activée sur l'appareil partenaire avec lequel le lag est formé. Une fois qu'un LAG automatique est formé, le commutateur applique automatiquement le mode réseau (c'est-à-dire un réseau automatique) au LAG aux deux extrémités. En d'autres termes, après la formation d'un auto-lag, le mode pour les ports qui participent à un auto-lag passe du mode de port de commutation par défaut au mode de port de jonction. Pour plus d'informations sur l'option Auto Ping Host, reportez-vous à la section .

Pour que le commutateur forme un réseau automatique avec un périphérique partenaire, les éléments suivants sont requis :

- Les fonctions Auto-lag et Auto-Trunk doivent être prises en charge et activées globalement sur le commutateur et l'appareil partenaire. (Sur le commutateur NETGEAR, les fonctions Auto-lag et Auto-Trunk sont activées par défaut.)
- Au moins deux liaisons doivent être établies entre le commutateur et le périphérique partenaire, et ces liaisons doivent prendre en charge la même vitesse et le même mode duplex.
- Les liens ne peuvent pas être membres d'un lag statique ou dynamique configuré manuellement.

- LLDP doit être activé sur les ports interconnectés sur le commutateur et le périphérique partenaire. (Sur le commutateur NETGEAR, LLDP est activé par défaut sur tous les ports.)
- Les ports interconnectés sur le commutateur et le périphérique partenaire doivent être en mode port de commutateur par défaut, qui est le mode général. Si les ports sont en mode accès ou déjà en mode réseau, un réseau automatique ne peut pas être formé sur un LAG automatique.

Un Auto-lag peut se former avec jusqu'à huit interfaces comme membres. Les interfaces sont automatiquement sélectionnées pour Auto-lag selon qu'elles sont actives et disponibles et selon les conditions suivantes :

- L'interface n'est pas déjà configurée manuellement en tant que membre d'un lag.
- L'interface n'est pas configurée manuellement en tant que port agrégé ou port d'accès. C'est-à-dire que l'interface doit être une interface générale.

❗ Remarque: Le commutateur peut prendre en charge plusieurs LAG statiques et dynamiques, mais avec chaque périphérique partenaire, le commutateur ne peut prendre en charge qu'un seul Auto-lag.

Activer ou désactiver les LAG automatiques

Par défaut, la fonction Auto-LAG est activée globalement, mais vous pouvez la désactiver globalement.

Pour activer ou désactiver les LAG automatiques :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > lag > Configuration lag**.

L'écran LAG Configuration (Configuration IP) s'affiche.

6. Dans la section Configuration globale lag, sélectionnez le bouton radio **Activer** ou **désactiver** le mode Admin Auto-lag.

Par défaut, la fonction Auto-LAG est activée.

7. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Activer ou désactiver le mode de profil AVB global Auto-lag

Le profil Audio vidéo AVB est l'un des profils réseau pris en charge par le contrôleur NETGEAR engage. Ce profil réseau peut être utilisé pour les périphériques audio IP prenant en charge le pontage audio vidéo (AVB). Par défaut, le mode profil AVB global Auto-lag est activé globalement, mais vous pouvez désactiver globalement informatique.

Pour activer ou désactiver le mode profil AVB global Auto-lag :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > lag > Configuration lag**.

L'écran LAG Configuration (Configuration IP) s'affiche.

6. Dans la section Configuration globale lag, sélectionnez le bouton radio **Activer** ou **désactiver** le mode profil AVB global Auto-lag.

Par défaut, le mode profil AVB global Auto-lag est activé globalement.

7. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez le mode de hachage pour les LAG automatiques

Par défaut, la fonction lag automatique est activée et utilise un mode de hachage qui configure automatiquement un lag en fonction de l'adresse MAC de destination, VLAN, EtherType et du port entrant dans le paquet (c'est-à-dire le mode de hachage avec le nom MAC de destination 2, VLAN, EType, port entrant). Vous pouvez modifier le mode de hachage (c'est-à-dire le mode d'équilibrage de charge) pour la fonction Auto-lag.

Le commutateur équilibre le trafic sur un lag en sélectionnant l'une des liaisons du canal sur lequel les paquets doivent être transmis. Le commutateur sélectionne la liaison en créant un motif binaire à partir de champs sélectionnés dans un paquet et en associant ce motif à une liaison particulière. Le mode hachage détermine les champs d'un paquet que le commutateur sélectionne.

Pour modifier le mode de hachage des LAG automatiques :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > lag > Configuration lag**.

L'écran LAG Configuration (Configuration IP) s'affiche.

6. Dans la section Configuration globale lag, dans le menu **mode de hachage global Auto-lag**, sélectionnez le mode de hachage pour les LAG automatiques :

- **1 SRC MAC, VLAN, EType, Port entrant** : Adresse MAC source, VLAN, EtherType et port entrant associés au paquet.
- **2 Dest MAC, VLAN, EType, Port entrant** : Adresse MAC de destination, VLAN, EtherType et port entrant associés au paquet. Il s'agit du mode par défaut.

- **3 SRC/destination MAC, VLAN, EType, Port entrant** : Adresses MAC source et de destination, VLAN, EtherType et port entrant associés au paquet.
 - **4 champs SRC IP et SRC TCP/UDP Port** : Champs adresse IP source et port TCP/UDP source du paquet.
 - **5 champs adresse IP destination et Port TCP/UDP destination** : Champs adresse IP de destination et port TCP/UDP de destination du paquet.
 - **6 champs SRC/Dest IP et TCP/UDP Port** : Adresses IP source et de destination et champs de port TCP/UDP source et de destination du paquet.
 - **7 mode de hachage amélioré** : Fonctionnement modulo-n (mod-n) basé sur le nombre de ports dans le lag, trafic non monodiffusion et hachage du trafic monodiffusion à l'aide d'un algorithme de hachage commun, excellentes performances d'équilibrage de charge et sélection des attributs de paquet en fonction du type de paquet :
 - Pour les paquets L2, l'adresse MAC source et l'adresse MAC de destination sont utilisées pour le calcul de hachage.
 - Pour les paquets L3, l'adresse IP source, l'adresse IP de destination et les ports TCP ou UDP sont utilisés pour le calcul de hachage.
7. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez le mode de hachage global non unicast

Un hachage est une chaîne de caractères de longueur fixe créée à partir d'un message ou de données plus longs. Le hachage est le processus de création d'un hachage, et une fonction de hachage est l'algorithme spécifique utilisé pour créer le hachage. Le mode de hachage global sans monodiffusion améliore l'équilibrage de charge pour le trafic sans monodiffusion, tel que les paquets multicast et broadcast. informatique permet aux périphériques réseau de distribuer le trafic non monodiffusion sur plusieurs liaisons dans un lag à l'aide d'un algorithme de hachage.

Pour modifier le mode de hachage pour le trafic non monodiffusion :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > lag > Configuration lag**.

L'écran LAG Configuration (Configuration IP) s'affiche.

6. Dans la section mode de hachage global sans monodiffusion, sélectionnez le mode de hachage pour le trafic sans monodiffusion :

- Port source Cochez la case **Port source** pour associer le numéro de port source au paquet.
- **Adresse MAC/IP source** : Cochez la case **adresse MAC/IP source** pour associer l'adresse MAC et l'adresse IP du port source au paquet. Par défaut, cette case est cochée.
- **Adresse MAC/IP de destination** : Cochez la case **adresse MAC/IP de destination** pour associer l'adresse MAC et l'adresse IP du port de destination au paquet. Par défaut, cette case est cochée.
- Améliorations : Cochez la case améliorée pour répartir uniformément le trafic non monodiffusion ou équilibrer la charge du trafic sur le lag. Par défaut, le mode amélioré est désactivé.

7. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez les paramètres d'un lag

Vous pouvez regrouper une ou plusieurs liaisons Ethernet full-duplex à agréger pour former un groupe d'agrégation de liaisons, également appelé port-Channel. Le commutateur traite le lag comme si le informatique était une liaison unique.

Pour configurer les paramètres d'un lag :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > lag > Configuration lag**.

L'écran LAG Configuration (Configuration IP) s'affiche.

6. Cochez la case d'un lag.

7. Pour modifier le nom par défaut du lag, dans le champ **nom du lag**, entrez le nom à attribuer au lag.

Par défaut, les noms sont ch1, ch2, ch3, etc. Vous pouvez entrer un nom de 15 caractères maximum.

Pour plus d'informations sur l'ajout d'un nom dans le champ Description, reportez-vous à la section [Ajoutez des descriptions de port, lag et VLAN](#) à la page 472 ou [Configurez un lag unique et ses membres](#) à la page 488.

8. Dans le menu **mode Admin**, sélectionnez pour activer ou désactiver le lag.
Lorsque le lag est désactivé, aucun flux de trafic et aucune LACPDU ne sont abandonnés, mais les liens qui forment le lag ne sont pas libérés. La valeur par défaut est Activer.
9. Dans le menu **mode de hachage**, sélectionnez le mode de hachage (c'est-à-dire le mode d'équilibrage de charge) pour le lag :
 - **1 SRC MAC, VLAN, EType, Port entrant** : Adresse MAC source, VLAN, EtherType et port entrant associés au paquet.
 - **2 Dest MAC, VLAN, EType, Port entrant** : Adresse MAC de destination, VLAN, EtherType et port entrant associés au paquet. Il s'agit du mode par défaut.
 - **3 SRC/destination MAC, VLAN, EType, Port entrant** : Adresses MAC source et de destination, VLAN, EtherType et port entrant associés au paquet.
 - **4 champs SRC IP et SRC TCP/UDP Port** : Champs adresse IP source et port TCP/UDP source du paquet.
 - **5 champs adresse IP destination et Port TCP/UDP destination** : Champs adresse IP de destination et port TCP/UDP de destination du paquet.
 - **6 champs SRC/Dest IP et TCP/UDP Port** : Adresses IP source et de destination et champs de port TCP/UDP source et de destination du paquet.
 - **7 mode de hachage amélioré** : Fonctionnement MODULO-N basé sur le nombre de ports dans le lag, trafic non monodiffusion et hachage du trafic monodiffusion à l'aide d'un algorithme de hachage commun, excellentes performances d'équilibrage de charge et sélection des attributs de paquet en fonction du type de paquet
 - Pour les paquets L2, l'adresse MAC source et l'adresse MAC de destination sont utilisées pour le calcul de hachage.
 - Pour les paquets L3, l'adresse IP source, l'adresse IP de destination et les ports TCP ou UDP sont utilisés pour le calcul de hachage.
- ❗ **Remarque:** Le commutateur équilibre le trafic sur un lag en sélectionnant l'une des liaisons du canal sur lequel les paquets doivent être transmis. Le commutateur sélectionne la liaison en créant un motif binaire à partir de champs sélectionnés dans un paquet et en associant ce motif à une liaison particulière. Le mode hachage détermine les champs d'un paquet que le commutateur sélectionne.
10. Dans le menu **mode STP**, sélectionnez pour activer ou désactiver le mode d'administration du protocole STP (Spanning Tree Protocol) pour le lag.
La valeur par défaut est Activer.

11. Dans le menu **mode statique**, sélectionnez pour activer ou désactiver le lag en tant que lag statique.

Lorsque le mode statique est activé, le lag ne transmet ni ne traite les LACPDU entrantes. Autrement dit, un port membre lag ne transmet pas de LACPDU et les LACPDU reçues par informatique sont abandonnées. La valeur par défaut est désactiver.

12. Dans le menu **lien interruption**, sélectionnez pour activer ou désactiver la transmission d'une interruption lorsque l'état de la liaison lag change.

La valeur par défaut est Activer, ce qui permet d'envoyer une interruption.

13. Dans le menu **mode préférence locale**, sélectionnez si le trafic monodiffusion connu envoyé au lag utilise uniquement l'interface lag de l'unité locale dans un environnement d'empilement :

- Activer. Ce mode est destiné à un environnement d'empilement. Si le lag est constitué de ports provenant des unités d'empilement, tout trafic monodiffusion *connu* envoyé au lag utilise uniquement l'interface lag sur l'unité locale. Activez ce mode pour vous assurer que le trafic de monodiffusion connu envoyé au lag ne traverse pas la liaison de pile externe lorsque le lag possède un ou plusieurs membres sur l'unité locale. Ce mode n'affecte pas le trafic unicast, broadcast et multicast *inconnu*.
- Désactiver : Le trafic de monodiffusion connu envoyé au lag n'est pas limité à l'interface lag de l'unité locale. Si vous n'utilisez pas la superposition, laissez ce mode désactivé, qui est le mode par défaut.

14. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

15. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 95 : Informations de configuration lag

Champ	Description
Description de l'LAG	La description que vous avez peut-être ajoutée à lag (voir Ajoutez des descriptions de port, lag et VLAN à la page 472 ou Configurez un lag unique et ses membres à la page 488)
ID LAG	L'identifiant lag
Ports configurés	Interfaces membres de lag
Ports d'arrêt	Les interfaces qui sont membres du lag mais qui sont en panne
Etat de lag	Indique si la liaison lag est active ou inactive

Table 95 : Informations de configuration lag (A continué)

Champ	Description
lag automatique	Indique si le lag est créé manuellement (non) ou automatiquement (Oui)
Mode profil AVB	Indique l'état opérationnel du mode profil AVB sur le lag

Configurez un lag unique et ses membres

Vous pouvez configurer un lag unique et ajouter des interfaces physiques en tant que membres du lag.

Les informations relatives à la configuration du lag sont identiques à celles de la [Configurez les paramètres d'un lag](#) à la page 485 section , mais les informations relatives à l'ajout de membres au lag sont uniques dans la section suivante.

Pour configurer un lag unique et son appartenance :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > lag > abonnement lag** .

La page adhésion à lag s'affiche.

6. Dans le menu **lag ID** to, sélectionnez lag.
7. Pour modifier le nom par défaut du lag, dans le champ **nom du lag**, entrez le nom à attribuer au lag.
Par défaut, les noms sont ch1, ch2, ch3, etc. Vous pouvez entrer un nom de 15 caractères maximum.
8. Pour entrer une description pour le lag, dans le champ **Description lag**, entrez une description de 64 caractères maximum.
9. Dans le menu **mode Admin**, sélectionnez pour activer ou désactiver le lag.
Lorsque le lag est désactivé, aucun flux de trafic et aucune LACPDU ne sont abandonnés, mais les liens qui forment le lag ne sont pas libérés. La valeur par défaut est Activer.
10. Dans le menu **Link Trap**, sélectionnez pour activer ou désactiver la transmission des interruptions lorsque l'état de la liaison lag change.
La valeur par défaut est désactiver, ce qui empêche l'envoi d'interruptions.
11. Dans le menu **mode STP**, sélectionnez pour activer ou désactiver le mode d'administration du protocole STP (Spanning Tree Protocol) pour le lag.
Activer est la valeur par défaut.
12. Dans le menu **mode statique**, sélectionnez pour activer ou désactiver le lag en tant que lag statique.
Lorsque le mode statique est activé, le lag ne transmet ni ne traite les LACPDU entrantes. Autrement dit, un port membre lag ne transmet pas de LACPDU et les LACPDU reçues par informatique sont abandonnées. La valeur par défaut est désactiver.
13. Dans le menu **mode de hachage**, sélectionnez le mode d'équilibrage de charge pour le lag :
 - **SRC MAC, VLAN, EType, Port entrant** : Adresse MAC source, VLAN, EtherType et port entrant associés au paquet.
 - **Destination MAC, VLAN, EType, port entrant** : Adresse MAC de destination, VLAN, EtherType et port entrant associés au paquet. Il s'agit du mode par défaut.
 - **SRC/destination MAC, VLAN, EType, Port entrant** : Adresses MAC source et de destination, VLAN, EtherType et port entrant associés au paquet.
 - **Champs SRC IP et SRC TCP/UDP Port** : Champs adresse IP source et port TCP/UDP source du paquet.
 - **Champs destination IP et destination TCP/UDP Port** : Champs adresse IP de destination et port TCP/UDP de destination du paquet.

- **Champs SRC/Dest IP et TCP/UDP Port** : Adresses IP source et de destination et champs de port TCP/UDP source et de destination du paquet.
- **Mode de hachage amélioré** : Fonctionnement MODULO-N basé sur le nombre de ports dans le lag, trafic non monodiffusion et hachage du trafic monodiffusion à l'aide d'un algorithme de hachage commun, excellentes performances d'équilibrage de charge et sélection des attributs de paquet en fonction du type de paquet
 - Pour les paquets L2, l'adresse MAC source et l'adresse MAC de destination sont utilisées pour le calcul de hachage.
 - Pour les paquets L3, l'adresse IP source, l'adresse IP de destination et les ports TCP ou UDP sont utilisés pour le calcul de hachage.

❗ **Remarque:** Le commutateur équilibre le trafic sur un lag en sélectionnant l'une des liaisons du canal sur lequel les paquets doivent être transmis. Le commutateur sélectionne la liaison en créant un motif binaire à partir de champs sélectionnés dans un paquet et en associant ce motif à une liaison particulière.

14. Dans le tableau ports, cliquez sur chaque port que vous souhaitez rendre membre du lag.

Si l'empilement est activé, un tableau ports s'affiche pour chaque commutateur de la pile.

15. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

16. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

802.1AS synchronisation et synchronisation

802.1AS synchronisation et synchronisation est une fonction de pontage audio vidéo (AVB).

La norme IEEE 802.1AS spécifie le protocole et les procédures utilisés pour garantir que les exigences QoS sont garanties pour les applications sensibles au facteur temps, telles que l'audio et la vidéo.

Le protocole IEEE 1588 Precision Time Protocol (PTP) constitue la base de la norme IEEE 802.1AS. PTP spécifie un protocole de synchronisation d'horloge précis qui repose sur des paquets horodatés. Pour plus d'informations sur la configuration du PTP,

reportez-vous aux sections [Horloge transparente a protocole temporel de PRECISION](#) à la page 136 et [Horloge limite de protocole de temps de précision et horloge grand maître](#) à la page 139.

Le protocole PTP est applicable à des systèmes distribués constitués d'un ou de plusieurs noeuds communiquant sur des supports de communication. La distribution des informations temporelles synchrones se fait de manière hiérarchique avec une horloge grand maître à la racine de la hiérarchie. Le grand maître fournit une référence temporelle commune et précise pour un ou plusieurs dispositifs directement connectés par échange périodique d'informations de synchronisation. C'est-à-dire que tous les appareils synchronisent leurs horloges avec l'horloge du grand maître. Les dispositifs peuvent, à leur tour, servir de dispositifs maîtres pour d'autres couches hiérarchiques d'autres dispositifs.

❗ Remarque: 802.1AS le pontage audio vidéo (AVB) n'est pas compatible avec l'empilement. Vous pouvez configurer l'un ou l'autre.

Configurer et afficher les paramètres 802.1AS globaux

Vous pouvez activer globalement 802.1AS sur le commutateur et configurer les priorités d'horloge locales. La fonction 802.1AS calcule le délai entre les périphériques d'une liaison et maintient une vue précise de l'horloge réseau.

Pour configurer et afficher les paramètres 802.1AS globaux sur le commutateur :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > 802.1AS > basique > Configuration 802.1AS**.

La page Configuration 802.1AS s'affiche.

6. Pour activer la fonction, sélectionnez le bouton radio **Activer** état 802.1AS.

7. Dans le champ **priorité de l'horloge locale1**, spécifiez la première valeur de priorité de l'horloge locale.

L'horloge locale est l'horloge du commutateur en tant que pont sensible au temps. Saisissez une valeur comprise entre 0 et 255. La valeur par défaut est de 255 secondes.

8. Dans le champ **priorité de l'horloge locale2**, spécifiez la deuxième valeur de priorité de l'horloge locale.

Saisissez une valeur comprise entre 0 et 255. La valeur par défaut est de 248 secondes.

9. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 96 : Informations de configuration 802.1AS

Champ	Description
Grandmaster capable	Indique si l'horloge du grand maître est active. La valeur par défaut est False.
Meilleure identité d'horloge	Adresse MAC de la meilleure horloge détectée par le commutateur.
Meilleure priorité horloge 1	La première valeur de priorité de la meilleure horloge détectée par le commutateur.

Table 96 : Informations de configuration 802.1AS (A continué)

Champ	Description
Meilleure priorité d'horloge 2	Deuxième valeur de priorité de la meilleure horloge détectée par le commutateur.
Étapes vers la meilleure horloge	Le nombre de liens entre la meilleure horloge et le commutateur. Si le commutateur lui-même est la meilleure horloge, la valeur est zéro.
Identité de l'horloge locale	Adresse MAC de l'horloge locale du commutateur.
Nombre de modifications GM	Le nombre de fois où l'horloge du grand maître a changé.
Horodatage de la dernière modification GM	Heure à laquelle le changement d'horloge grand maître le plus récent s'est produit.

Configurez les paramètres de l'interface 802.1AS

Vous pouvez configurer les paramètres 802.1AS pour des interfaces individuelles.

Pour configurer les paramètres de l'interface 802.1AS :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **commutation > 802.1AS > Avancé > Paramètres de port 802.1AS**.
La page Paramètres du port 802.1AS s'affiche.
6. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :
 - **1 ou ID d'unité pour un commutateur empilé :**
 - 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
 - **ID d'unité pour un commutateur empilé :** Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
 - **LAG** Seuls les LAG sont affichés.
 - **Tous:** Les interfaces physiques et les LAG sont affichés, ou pour une pile de commutateurs, les interfaces physiques de tous les commutateurs de la pile et les LAG sont affichés.
7. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :
 - Pour afficher ou effacer les statistiques d'une seule interface, cochez la case associée à l'interface ou saisissez le numéro de l'interface dans le champ **aller à l'interface** et cliquez sur le bouton **aller**.
 - Pour configurer plusieurs interfaces avec les mêmes paramètres, cochez la case associée à chaque interface.
 - Pour configurer toutes les interfaces avec les mêmes paramètres, cochez la case dans la ligne d'en-tête.
8. Dans le menu du mode EEE, sélectionnez Activer ou désactiver.
Pour que les paramètres 802.1AS prennent effet sur l'interface, sélectionnez **Activer**.
La valeur par défaut est désactiver.
9. Dans le champ **seuil Pdelay**, spécifiez le seuil de délai de propagation pour l'interface.

Le seuil détermine si le port est capable de participer au protocole 802.1AS. Si le délai de propagation sur l'interface est supérieur au seuil que vous configurez, l'interface n'est pas considérée comme capable de participer au protocole 802.1AS. Le délai homologue doit être inférieur à la valeur de seuil configurée sur l'interface. La plage est comprise entre 0 et 1 000 000 000 nanosecondes (ns). La valeur par défaut est 2500 ns.

10. Dans le champ **réponses perdues autorisées**, spécifiez la valeur de réponse **perdue** autorisée.

Si l'interface ne reçoit pas de réponses valides aux messages PDELAY_REQ au-dessus de la valeur des réponses perdues autorisées, un port est considéré comme n'échangeant pas de messages de retard pair avec son voisin. La plage est de 0 à 65 535. Le numéro par défaut est 3.

11. Dans le champ **Interva de synchronisation initiale**, spécifiez le taux de transmission des messages DE SYNCHRONISATION.

Cette valeur est le logarithme en base 2 de l'intervalle de temps moyen entre les messages DE SYNCHRONISATION successifs émis sur cette interface. L'intervalle initial configuré devient l'intervalle actuel uniquement après l'initialisation ou la réinitialisation du port pour le fonctionnement 802.1AS. La plage est de -5 à 5. Le numéro par défaut est -3.

12. Dans le champ **intervalle Pdelay initial**, spécifiez le taux de transmission des messages PDELAY_REQ.

Cette valeur est le logarithme en base 2 de l'intervalle de temps moyen entre les messages PDELAY_REQ successifs émis sur cette interface. L'intervalle initial configuré devient l'intervalle actuel uniquement après l'initialisation ou la réinitialisation du port pour le fonctionnement 802.1AS. La plage est de -5 à 5. Le numéro par défaut est -3.

13. Dans le champ **intervalle d'annonce initial**, spécifiez le taux de transmission des messages D'ANNONCE.

Cette valeur est le logarithme en base 2 de l'intervalle de temps moyen entre les messages D'ANNONCE successifs émis sur cette interface. L'intervalle initial configuré devient l'intervalle actuel uniquement après l'initialisation ou la réinitialisation du port pour le fonctionnement 802.1AS. La plage est de -5 à 5. Le numéro par défaut est -3.

14. Dans le champ **SyncRx Timeout**, spécifiez le nombre d'intervalles DE SYNCHRONISATION.

Cette valeur définit le nombre d'intervalles DE SYNCHRONISATION qui doivent passer sans réception d'informations DE SYNCHRONISATION avant que le commutateur ne détecte que l'horloge maître n'est plus en train de transmettre.

15. n dans le champ **délai d'annonce Rx**, spécifiez le nombre d'intervalles D'ANNONCE.

Cette valeur définit le nombre d'intervalles D'ANNONCE qui doivent s'écouler sans réception de l'ANNONCE PDU avant que le commutateur ne détecte que l'horloge maître n'est plus en train de transmettre.

16. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

17. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 97 : Informations sur l'interface 802.1AS

Champ	Description
Rôle du port	Rôle 802.1AS de l'interface. Les rôles possibles sont les suivants : • Désactivée (défaut) • Maître • Esclave • Passif
Délai de propagation	Le temps de propagation moyen sur l'interface.
Mesure de Pdelay	Indique si l'interface reçoit des messages de réponse PDELAY de l'autre extrémité de la liaison.
Compatible 802.1AS	Indique si l'interface est compatible 802.1AS. Par défaut, l'interface n'est pas compatible 802.1AS.
Taux voisin	Un rapport estimé de la fréquence de l'entité d'horloge locale du dispositif sensible au temps à l'autre extrémité de la liaison de l'interface par rapport à la fréquence de l'entité d'horloge locale du commutateur.
Intervalle de synchronisation actuel	Intervalle de temps moyen courant entre les messages DE SYNCHRONISATION successifs envoyés sur la liaison, en format logarithme en base 2.
Intervalle Pdelay actuel	Intervalle de temps moyen courant entre les messages PDELAY_REQ successifs envoyés sur la liaison, au format logarithme en base 2.
Intervalle d'annonce actuel	Intervalle de temps moyen courant entre les messages D'ANNONCE successifs envoyés sur la liaison, en format logarithme en base 2.

Afficher les statistiques 802.1AS

Vous pouvez afficher les statistiques 802.1AS pour les interfaces.

Pour afficher les statistiques 802.1AS pour les interfaces :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > 802.1AS > Avancé > statistiques 802.1AS**.

6. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :

- 1. Seules les interfaces physiques sont affichées. Il s'agit de l'option par défaut.
- LAG Seuls les LAG sont affichés.
- **Tous:** Les interfaces physiques et les LAG sont affichés.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 98 : 802.1AS informations statistiques

Champ	Description
Interface	Interface pour laquelle les informations sont affichées.
Sync Tx	Nombre total de paquets DE SYNCHRONISATION transmis sans erreur.
Sync Rx	Nombre total de paquets DE SYNCHRONISATION reçus sans erreur.
Suivi Tx	Nombre total de paquets FOLLOWUP transmis sans erreur.
Suivi Rx	Nombre total de paquets FOLLOWUP reçus sans erreur.
Annoncer Tx	Nombre total de paquets D'ANNONCE transmis sans erreur.
Annoncer Rx	Nombre total de paquets D'ANNONCE reçus sans erreur.
Pdelay req Tx	Nombre total de paquets PDELAY_REQ transmis sans erreur.
Pdelay Req Rx	Nombre total de paquets PDELAY_REQ reçus sans erreur.

Table 98 : 802.1AS informations statistiques (A continué)

Champ	Description
Pdelay Resp Tx	Nombre total de paquets PDELAY_RESP transmis sans erreur.
Pdelay Resp Rx	Nombre total de paquets PDELAY_RESP reçus sans erreur.
Pdelay Resp Followup Tx	Nombre total de paquets PDELAY_RESP_FOLLOWUP transmis sans erreur.
Pdelay Resp Followup Rx	Nombre total de paquets PDELAY_RESP_FOLLOWUP reçus sans erreur.
Signalisation Tx	Nombre total de paquets de SIGNALISATION transmis sans erreur.
Signalisation Rx	Nombre total de paquets de SIGNALISATION reçus sans erreur.
Délais de synchronisation	Nombre total de délais d'expiration de réception de SYNCHRONISATION qui se sont produits.
Synchronisez les rejets	Nombre total de paquets DE SYNCHRONISATION qui ont été rejetés.
Annoncer les délais d'expiration	Nombre total de délais D'expiration D'ANNONCE de réception qui se sont produits.
Annoncer les rejets	Nombre total de paquets D'ANNONCE qui ont été rejetés.
Temporisations Pdelay	Nombre total de dépassements de délai de réception PDELAY qui se sont produits.
Rejets Pdelay	Nombre total de paquets PDELAY rejetés.
En-têtes défectueux	Nombre total de paquets reçus avec un en-tête incorrect.

Protocole d'enregistrement multiple et 802.1Qav

Multiple Registration Protocol (MRP) est une fonction de pontage audio vidéo (AVB). MVR est un protocole d'enregistrement de base qui permet aux périphériques exécutant une application MRP d'enregistrer des attributs sur d'autres périphériques d'un réseau. MRP fournit une application pour enregistrer des attributs tels que la bande passante pour un flux audio-vidéo (AV) et les informations d'adresse MAC. Cette fonction est utilisée par diverses applications pour propager l'enregistrement.

❗ Remarque: La structure MRP doit être disponible et activée sur tous les périphériques intermédiaires afin de garantir que la propagation des attributs se produit sur l'ensemble du réseau.

Le commutateur prend en charge les applications MRP suivantes :

- **Protocole d'enregistrement MAC multiple (MMRP)** : MMRP permet la propagation des informations d'adresse MAC dans le réseau, et permet l'enregistrement et le désenregistrement des informations d'adresse MAC individuelles et de l'appartenance à une adresse MAC de groupe. Les stations terminales peuvent demander à rejoindre ou quitter un groupe de multidiffusion, ou à enregistrer une adresse MAC individuelle avec un VLAN spécifique. Les entrées d'adresse MAC peuvent être enregistrées et désenregistrées dynamiquement si MMRP est activé administrativement sur le commutateur.
- **Protocole d'enregistrement multiple VLAN (MVRP)** : MVRP enregistre les VLAN dans le réseau, ce qui permet la configuration automatique des VLAN sur le commutateur. Dans un réseau typique, le marquage VLAN est courant. De nombreux nœuds nécessitent que le trafic d'entrée soit étiqueté avec un ID VLAN spécifique, et d'autres nœuds nécessitent que le trafic de sortie soit transmis avec un ID VLAN spécifique. Avec l'utilisation de MVRP à la fois en entrée et en sortie, aucune configuration VLAN manuelle n'est requise pour faire passer le trafic balisé sur le réseau.
- **Protocole de réservation de flux multiples (MSRP)** : MSRP réserve des ressources dans le réseau pour faciliter le trafic sensible au temps pour circuler de bout en bout. Un réseau typique comprend plusieurs émetteurs (périphériques qui transmettent des flux) et plusieurs récepteurs (périphériques qui reçoivent des flux d'un ou plusieurs émetteurs). Chaque flux a des exigences spécifiques en matière de bande passante, de fréquence d'images et de synchronisation temporelle. MSRP garantit ces ressources via tous les périphériques intermédiaires entre n'importe quel locuteur et écouteur.

Avec MRP, les attributs réseau sont déclarés, enregistrés, retirés et supprimés dynamiquement sans intervention de l'utilisateur. Cette nature dynamique est particulièrement utile dans les réseaux où ce qui suit est vrai :

- Les attributs réseau sont susceptibles de changer fréquemment, ce qui nécessite une reconfiguration des périphériques intermédiaires.
- Les bénéficiaires de ces attributs augmentent ou diminuent fréquemment en nombre.
- Chacun de ces changements sans cadre dynamique d'auto-ajustement exigerait une attention constante de la part d'un administrateur réseau.

Configurez les paramètres MRP globaux

Vous pouvez configurer les paramètres MRP globaux pour le commutateur.

Pour configurer les paramètres MRP globaux :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > MRP > basique > Configuration MRP**.

L'écran MRP Configuration (Configuration IP) s'affiche.

6. Sélectionnez le bouton radio **Activer** ou **désactiver** le mode MVRP pour spécifier le mode d'administration global de MVRP sur le commutateur.

L'activation de ce mode permet à MVRP d'enregistrer des VLAN dans le réseau, ce qui permet la configuration automatique de VLAN sur le périphérique. La valeur par défaut est désactiver.

7. Sélectionnez le bouton radio **Activer** ou **désactiver** MMRP pour spécifier le mode d'administration global de MMRP sur le commutateur.

L'activation de ce mode permet la propagation des informations d'adresse MAC dans le réseau. À son tour, cela permet l'enregistrement et le désenregistrement des informations d'adresse MAC individuelles et de l'appartenance à une adresse MAC de groupe. La valeur par défaut est désactiver.

8. Sélectionnez le bouton radio **Activer** ou **désactiver le** PDSF pour spécifier le mode d'administration global du PDSF sur le commutateur.

L'activation de ce mode permet au commutateur de réserver des ressources dans le réseau afin de faciliter le flux du trafic sensible au temps de bout en bout. La valeur par défaut est désactiver.

9. Sélectionnez le bouton radio **Activer** ou **désactiver** l'élagage de l'avertisseur PDSF.

L'activation de ce mode limite le commutateur à la transmission d'unités de données de protocole d'émetteur (PDU) aux adresses MAC de destination qui se trouvent dans la MFDB (Multicast Forwarding table). Une PDU de locuteur est la source d'un flux audio-vidéo. La valeur par défaut est désactiver.

10. Sélectionnez le bouton radio Periodic State machine (mode MVRP) **Activer** ou **désactiver**.

L'activation de ce mode peut limiter l'effet des modifications de topologie MVRP et réduire le nombre de PDU transmises entre les périphériques. La valeur par défaut est désactiver.

11. Sélectionnez le bouton radio Periodic State machine (MMRP) **Activer** ou **désactiver**.

L'activation de ce mode peut limiter l'effet des modifications de topologie MMRP et réduire le nombre d'unités de données de protocole (PDU) transmises entre les périphériques. La valeur par défaut est désactiver.

12. Dans le champ **ventilateur max. PDSF dans les ports**, spécifiez le nombre maximal d'interfaces sur lesquelles les enregistrements PDSF sont autorisés.

La plage dépend du modèle de commutateur. La valeur par défaut est 0, ce qui signifie qu'aucune limite n'est imposée sur le nombre d'interfaces.

13. Sélectionnez le bouton radio **Activer** ou **désactiver** la propagation des limites du PDSF.

Lorsque vous activez la propagation des limites du PDSF, selon la configuration, une réservation de flux peut être autorisée à traverser un port limite.

La valeur par défaut est désactiver.

14. Dans le champ **intervalle de temps de transmission PDU PDU PDU PDU**, spécifiez la période entre le transfert de deux PDU PDU PDU consécutives après l'expiration du délai LeaveAll.

Après expiration du délai LeaveAll, tous les participants sont désinscrits et doivent se joindre à nouveau en répondant aux PDU envoyées par le commutateur. En envoyant des PDU MSRP consécutives à intervalles réguliers, le tampon de paquets d'un point final récepteur ne débordera pas. La période entre deux PDU PDU PDU consécutives est une valeur en millisecondes.

15. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

16. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurer le mappage 802.1Qav

Vous pouvez définir les paramètres IEEE 802.1Qav globaux, qui sont des priorités QoS pour les flux audio vidéo Ethernet (EAV) de trafic de classe A et de classe B.

La norme IEEE 802.1Qav prend en charge les flux de trafic sensibles au temps en régulant l'ensemble du trafic du commutateur, y compris le trafic Ethernet asynchrone hérité, via la mise en file d'attente et le transfert. Lorsqu'un locuteur déclare un flux, 802.1Qav identifie si le flux est de classe A ou de classe B et spécifie les exigences de bande passante du flux. Le trafic de classe A reçoit une priorité de transmission plus élevée que le trafic de classe B.

Pour modifier les priorités de mappage 802.1Qav globales :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > MRP > basique > Configuration MRP**.

L'écran MRP Configuration (Configuration IP) s'affiche.

6. Faites défiler jusqu'à la section mappage 802.1qav.

Par défaut, la priorité EAV pour le trafic de classe A est 3, avec une priorité de remappage de 0.

Par défaut, la priorité EAV pour le trafic de classe B est 2, avec une priorité de remappage de 0.

7. Dans la colonne flux EAV, cochez la case de la classe.
8. Dans le champ **priorité EAV**, spécifiez une priorité comprise entre 0 et 7.
La priorité 0 est la priorité la plus basse ; la priorité 7 est la priorité la plus élevée.
9. Dans le champ **EAV Remap Priority**, spécifiez une priorité comprise entre 0 et 7.
La priorité 0 est la priorité la plus basse ; la priorité 7 est la priorité la plus élevée.
10. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
11. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez les paramètres de l'interface MRP

Vous pouvez configurer le mode MRP et les paramètres de minuterie pour une ou plusieurs interfaces. Les minuteries contrôlent quand et à quelle fréquence les différents messages sont transmis sur chaque interface.

Pour configurer les paramètres de l'interface MRP :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > MRP > Avancé > Paramètres de port MRP**.

La page Paramètres du port MRP s'affiche.

6. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :

- **1 ou ID d'unité pour un commutateur empilé :**
 - 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
 - **ID d'unité pour un commutateur empilé :** Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
- **LAG** Seuls les LAG sont affichés.
- **Tous:** Les interfaces physiques et les LAG sont affichés, ou pour une pile de commutateurs, les interfaces physiques de tous les commutateurs de la pile et les LAG sont affichés.

7. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :

- Pour afficher ou effacer les statistiques d'une seule interface, cochez la case associée à l'interface ou saisissez le numéro de l'interface dans le champ **aller à l'interface** et cliquez sur le bouton **aller**.
- Pour configurer plusieurs interfaces avec les mêmes paramètres, cochez la case associée à chaque interface.
- Pour configurer toutes les interfaces avec les mêmes paramètres, cochez la case dans la ligne d'en-tête.

8. Dans le menu **mode MVRP**, sélectionnez **Activer** ou **désactiver** pour spécifier le mode d'administration de MVRP sur l'interface.

L'activation de ce mode permet à MVRP d'enregistrer des VLAN dans le réseau, ce qui permet la configuration automatique de VLAN sur l'interface. La valeur par défaut est désactiver.

9. Dans le menu **mode MMRP**, sélectionnez **Activer** ou **désactiver** pour spécifier le mode d'administration de MMRP sur l'interface.

L'activation de ce mode permet la propagation des informations d'adresse MAC sur l'interface. À son tour, cela permet l'enregistrement et le désenregistrement des informations d'adresse MAC individuelles et de l'appartenance à une adresse MAC de groupe. La valeur par défaut est désactiver.

10. Dans le menu **mode PDSF**, sélectionnez **Activer** ou **désactiver** pour spécifier le mode d'administration du PDSF sur l'interface.

L'activation de ce mode permet à l'interface de réserver des ressources dans le réseau afin de faciliter le flux du trafic sensible au temps de bout en bout. La valeur par défaut est désactiver.

11. Dans le champ **minuteur de jointure**, spécifiez le temps pendant lequel l'interface doit attendre les messages de jointure des autres participants MRV après l'envoi d'un message de jointure par l'interface.

Si le temps que vous spécifiez s'écoule avant que l'interface ne reçoive un message de jointure, l'interface renvoie le message de jointure. La plage est de 10 à 100 secondes. Le numéro par défaut est 20.

12. Dans le champ **délai de sortie**, spécifiez le délai d'attente de l'interface avant que informatique annule les attributs des autres participants MRV.

Si l'interface reçoit des messages de jointure d'autres participants avant l'expiration de l'heure spécifiée, les attributs ne sont pas désenregistrés. La plage est de 20 à 600 secondes. Le numéro par défaut est 100.

13. Dans le champ **laisser tous les minuteurs**, spécifiez le délai d'attente de l'interface après que informatique ait démarré le processus d'enregistrement MRP avant que les participants actualisent et réenregistrent leurs attributs.

La plage est comprise entre 200 et 6000 centisecondes. La valeur par défaut est 1000.

14. Dans le champ **PVID de la classe SR MSRP**, spécifiez l'ID VLAN par défaut que l'interface doit utiliser pour le trafic de flux MSRP.

15. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

16. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 99 : Informations sur les paramètres de l'interface MRP

Champ	Description
PDSF Port limite classe A.	Indique si l'interface est un port limite pour le trafic de classe A.
PDSF Port limite classe B.	Indique si l'interface est un port limite pour le trafic de classe B.

Afficher ou effacer les statistiques MMRP

Vous pouvez afficher ou effacer les informations relatives aux trames MMRP transmises et reçues par le commutateur et par chaque interface.

Pour afficher ou effacer les statistiques MMRP :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > MRP > Avancé > statistiques MMRP**.

La page statistiques MMRP s'affiche.

6. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :
 - **1 ou ID d'unité pour un commutateur empilé :**
 - 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
 - **ID d'unité pour un commutateur empilé :** Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
 - **LAG** Seuls les LAG sont affichés.
 - **Tous:** Les interfaces physiques et les LAG sont affichés, ou pour une pile de commutateurs, les interfaces physiques de tous les commutateurs de la pile et les LAG sont affichés.
7. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).
8. Pour effacer les statistiques, procédez comme suit :
 - a. Cochez la case en regard de l'interface ou des interfaces ou, pour effacer les statistiques de toutes les interfaces, cochez la case dans l'en-tête du tableau.
 - b. Cliquez sur le bouton **Clear** (Effacer).

Les statistiques sont effacées.

9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 100 : Informations statistiques MMRP

Champ	Description
Statistiques globales MMRP	
Trames reçues	Nombre de trames MMRP reçues sur le commutateur.
En-tête incorrect	Nombre de trames MMRP avec des en-têtes défectueux reçues sur le commutateur.
Format incorrect	Nombre de trames MMRP avec des formats de corps PDU erronés qui ont été reçues sur le commutateur.
Trames transmises	Nombre de trames MMRP transmises sur le commutateur.
Défaillances de la transmission	Nombre de trames MMRP que le commutateur n'a pas transmises.
Statistiques MMRP	
Interface	Interface pour laquelle les informations sont affichées.
Trames reçues	Nombre de trames MMRP reçues sur l'interface.

Table 100 : Informations statistiques MMRP (A continué)

Champ	Description
En-tête incorrect	Nombre de trames MMRP avec des en-têtes erronés reçues sur l'interface.
Format incorrect	Nombre de trames MMRP avec des formats de corps PDU erronés qui ont été reçues sur l'interface.
Trames transmises	Nombre de trames MMRP transmises sur l'interface.
Défaillances de la transmission	Nombre de trames MMRP que l'interface n'a pas pu transmettre.

Afficher ou effacer les statistiques MVRP

Vous pouvez afficher ou effacer des informations sur les trames MVRP transmises et reçues par le commutateur et par chaque interface.

Pour afficher ou effacer les statistiques MVRP :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > MRP > Avancé > statistiques MVRP** .

La page statistiques MVRP s'affiche.

6. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :

- **1 ou ID d'unité pour un commutateur empilé :**
 - 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
 - **ID d'unité pour un commutateur empilé :** Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
- **LAG** Seuls les LAG sont affichés.
- **Tous:** Les interfaces physiques et les LAG sont affichés, ou pour une pile de commutateurs, les interfaces physiques de tous les commutateurs de la pile et les LAG sont affichés.

7. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

8. Pour effacer les statistiques, procédez comme suit :

- a. Cochez la case en regard de l'interface ou des interfaces ou, pour effacer les statistiques de toutes les interfaces, cochez la case dans l'en-tête du tableau.
- b. Cliquez sur le bouton **Clear** (Effacer).

Les statistiques sont effacées.

9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 101 : Informations statistiques MVRP

Champ	Description
Statistiques globales MVRP	
Trames reçues	Nombre de trames MMRP reçues sur le commutateur.
En-tête incorrect	Nombre de trames MMRP avec des en-têtes défectueux reçues sur le commutateur.
Format incorrect	Nombre de trames MMRP avec des formats de corps PDU erronés qui ont été reçues sur le commutateur.
Trames transmises	Nombre de trames MMRP transmises sur le commutateur.
Défaillances de la transmission	Nombre de trames MMRP que le commutateur n'a pas transmises.
Echec de la file d'attente des messages	Nombre de messages MMRP qui n'ont pas été ajoutés à la file d'attente.

Table 101 : Informations statistiques MVRP (A continué)

Champ	Description
Statistiques MVRP	
Interface	Interface pour laquelle les informations sont affichées.
Trames reçues	Nombre de trames MVRP reçues sur l'interface.
En-tête incorrect	Nombre de trames MVRP avec des en-têtes erronés reçues sur l'interface.
Format incorrect	Nombre de trames MVRP avec des formats de corps PDU erronés qui ont été reçues sur l'interface.
Trames transmises	Nombre de trames MVRP transmises sur l'interface.
Défaillances de la transmission	Nombre de trames MVRP que l'interface n'a pas pu transmettre.
Echec de l'enregistrement	Nombre de trames MVRP qui n'ont pas pu être enregistrées sur un périphérique ou une interface particulière.

Afficher ou effacer les statistiques du PDSF

Vous pouvez afficher ou effacer des informations sur les trames MSRP transmises et reçues par le commutateur et par chaque interface.

Pour afficher ou effacer les statistiques du PDSF :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > MRP > Avancé > statistiques PDSF**.

La page statistiques du PDSF s'affiche.

6. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :

- **1 ou ID d'unité pour un commutateur empilé :**
 - 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
 - **ID d'unité pour un commutateur empilé :** Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
- **LAG** Seuls les LAG sont affichés.
- **Tous:** Les interfaces physiques et les LAG sont affichés, ou pour une pile de commutateurs, les interfaces physiques de tous les commutateurs de la pile et les LAG sont affichés.

7. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

8. Pour effacer les statistiques, procédez comme suit :

- a. Cochez la case en regard de l'interface ou des interfaces ou, pour effacer les statistiques de toutes les interfaces, cochez la case dans l'en-tête du tableau.
- b. Cliquez sur le bouton **Clear** (Effacer).

Les statistiques sont effacées.

9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 102 : Informations statistiques sur le PDSF

Champ	Description
PDSF statistiques globales	
Trames reçues	Nombre de trames MSRP reçues sur le commutateur.
En-tête incorrect	Nombre de trames PDSF avec des en-têtes défectueux reçues sur le commutateur.
Format incorrect	Nombre de trames MSRP avec des formats de corps PDU erronés qui ont été reçues sur le commutateur.
Trames transmises	Nombre de trames MSRP transmises sur le commutateur.
Défaillances de la transmission	Nombre de trames MSRP que le commutateur n'a pas transmises.
Échecs de message	Nombre de messages PDSF qui n'ont pas été ajoutés à la file d'attente.
Statistiques du PDSF	
Interface	Interface pour laquelle les informations sont affichées.
Trames reçues	Nombre de trames MSRP reçues par l'interface.
En-tête incorrect	Nombre de trames MSRP avec un en-tête incorrect reçues sur l'interface.
Format incorrect	Nombre de trames MSRP avec un format de corps PDU incorrect reçues sur l'interface.
Trames transmises	Nombre de trames MSRP transmises sur l'interface.
Défaillances de la transmission	Nombre de trames MSRP que l'interface n'a pas pu transmettre.
Echec de l'enregistrement	Nombre de trames MSRP qui n'ont pas pu être enregistrées sur un périphérique ou une interface particulière.

Afficher les paramètres de réservation du PDSF

Vous pouvez afficher des informations sur l'état de l'émetteur, de l'écouteur et du périphérique intermédiaire pour les périphériques impliqués dans chaque flux MSRP qui passe par le commutateur.

Pour afficher les paramètres de réservation du PDSF :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > MRP > Avancé > Paramètres de réservation PDSF**.

La page Paramètres de réservation PDSF s'affiche.

6. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

Le tableau suivant décrit les champs en lecture seule de la page.

Table 103 : Informations sur les paramètres de réservation du PDSF

Champ	Description
Interface	Interface pour laquelle les informations sont affichées.
ID de flux	Une valeur entière non signée de 16 bits, qui est un ID unique utilisé pour distinguer le flux parmi plusieurs flux provenant du même périphérique.
Statut de déclaration de l'écouteur	État de déclaration MSRP de l'attribut d'écouteur.
Type de déclaration d'écouteur	Type de déclaration MSRP de l'attribut d'écouteur.
Statut de déclaration de l'intervenant	État de déclaration MSRP de l'attribut de l'émetteur.

Table 103 : Informations sur les paramètres de réservation du PDSF (A continué)

Champ	Description
Type de déclaration de l'intervenant	Le type de déclaration MSRP de l'attribut d'émetteur.
Latence accumulée	Latence, en nanosecondes, qui s'est produite pour le flux sur son chemin de l'émetteur à un écouteur. La latence commence par zéro et est augmentée de un pour chaque périphérique via lequel le flux se propage dans le réseau.
Défaillance de l'interface de pont	En cas de panne, l'interface sur le périphérique sur lequel la panne s'est produite.
Échec du pont MAC	En cas de panne, adresse MAC du périphérique sur lequel la panne s'est produite.
Code de défaillance	Si une défaillance s'est produite, le numéro qui représente la raison de la défaillance. Le commutateur prend en charge les codes suivants : • 1 : Bande passante insuffisante • 3 : Bande passante insuffisante pour la classe de trafic • 5 : L'adresse de destination du flux est déjà utilisée • 7 : Latence signalée modifiée • 8 : Le port de sortie n'est pas compatible avec le pontage audio/vidéo (AVB) • 9 : Utilisez une adresse de destination différente (par exemple, si la table de hachage MAC DA est pleine) • 12 : Impossible de stocker l'adresse de destination (par exemple, si le périphérique n'a plus de ressources MAC DA) • 13 : La priorité demandée n'est pas une priorité de classe SR • 14 : MaxFrameSize est trop grand pour le support • 15 : la limite de msrpMaxFanInPorts a été atteinte • 16 : Modifications de FirstValue pour un StreamID enregistré • 17 : VLAN est bloqué sur ce port de sortie (enregistrement interdit)
Âge du flux	Temps, en secondes, depuis que l'adresse de destination du flux a été ajoutée à la table entrées de réservations dynamiques. Une valeur de zéro indique que l'adresse de destination n'a pas été ajoutée à la table.

Configurer et afficher les paramètres Qav pour les interfaces

Vous pouvez configurer et afficher les paramètres IEEE 802.1Qav pour les interfaces. La norme IEEE 802.1Qav prend en charge les flux de trafic sensibles au temps en régulant l'ensemble du trafic du commutateur, y compris le trafic Ethernet asynchrone hérité, via la mise en file d'attente et le transfert. Lorsqu'un locuteur déclare un flux, 802.1Qav

identifie si le flux est de classe A ou de classe B et spécifie les exigences de bande passante du flux. Le trafic de classe a reçoit une priorité de transmission plus élevée que le trafic de classe B.

Vous pouvez configurer et afficher les allocations de bande passante sélectionnées pour le trafic de classe A et de classe B.

Pour configurer et afficher les paramètres Qav des interfaces :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > MRP > Avancé > Paramètres Qav** .

La page Paramètres Qav s'affiche.

6. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :

- Pour configurer une interface unique, cochez la case associée à l'interface.
- Pour configurer plusieurs interfaces avec les mêmes paramètres, cochez la case associée à chaque interface.
- Pour configurer toutes les interfaces avec les mêmes paramètres, cochez la case dans la ligne d'en-tête.

7. Dans le champ **bande passante delta MSRP** de classe A, spécifiez la bande passante supplémentaire représentée sous forme de pourcentage du débit de transmission de l'interface réservé au trafic de classe A et de classe B.

Le trafic de classe A reçoit une priorité plus élevée que le trafic de classe B. La plage est de 0 à 100. Le numéro par défaut est 100.

8. Dans le champ **bande passante delta MSRP** de classe B, spécifiez la bande passante supplémentaire représentée sous forme de pourcentage du débit de transmission de l'interface réservé au trafic de classe B.

La plage est de 0 à 100. Le numéro par défaut est 0.

9. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 104 : Informations sur les paramètres Qav

Champ	Description
Bande passante de classe A allouée	Débit actuel (en BPS) du trafic de classe A sur l'interface
Bande passante restante de classe A.	Débit maximal (en BPS) de classe A pris en charge par l'interface.
Bande passante de classe B allouée	Débit actuel (en BPS) du trafic de classe B sur l'interface
Bande passante restante de classe B.	Débit maximal (en BPS) de classe B pris en charge par l'interface.
Bande passante totale allouée	Somme des débits de trafic de classe A et de classe B alloués (en BPS) sur l'interface.
Bande passante totale restante	75 % de la vitesse de l'interface moins la bande passante allouée totale (en BPS/sec).

Afficher les informations sur les flux PDSF

Vous pouvez afficher des informations sur les flux MSRP qui circulent dans chaque interface.

Pour afficher les renseignements sur les flux PDSF :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > MRP > Avancé > informations flux PDSF**.

La page informations sur les flux PDSF s'affiche.

6. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

Le tableau suivant décrit les champs en lecture seule de la page.

Table 105 : Le PDSF diffuse des informations

Champ	Description
ID de flux	Une valeur entière non signée de 16 bits, qui est un ID unique utilisé pour distinguer le flux parmi plusieurs flux provenant du même périphérique
Adresse MAC source du flux	Adresse MAC de la source du flux de trafic
Latence accumulée reçue	Valeur de latence accumulée non signée de 32 bits qui est utilisée pour déterminer la latence la plus défavorable qu'un flux peut subir dans son chemin de l'émetteur à un écouteur. La latence commence par zéro et est augmentée de un pour chaque périphérique via lequel le flux se propage dans le réseau.
Classe de trafic	Indique si le flux est de classe A ou B. le trafic de classe A reçoit une priorité plus élevée que le trafic de classe B.

Table 105 : Le PDSF diffuse des informations (A continué)

Champ	Description
Ordre :	Valeur de rang 5 bits non signée utilisée par les périphériques pour déterminer quels flux peuvent encore être servis lorsque les enregistrements MSRP dépassent la capacité d'une interface à transporter les flux de données correspondants. Si un périphérique est sursouscrit (par exemple, une reconfiguration du réseau ou une réduction de bande passante de 802,11), la valeur de rang est également utilisée pour déterminer le flux abandonné. Une valeur numérique inférieure est plus importante qu'une valeur numérique supérieure.
Taille de trame max. TSPEC	Valeur de bande passante non signée de 32 bits utilisée pour allouer des ressources et ajuster les paramètres de sélection de file d'attente afin de fournir la qualité de service demandée par un locuteur MSRP. La valeur représente le débit maximal, en unités de 1024 octets par seconde, auquel des trames du flux référencé par le locuteur peuvent être transmises.
Trames d'intervalle max. TSPEC	Valeur de débit de trames non signées de 32 bits utilisée pour allouer des ressources et ajuster les paramètres de sélection de file d'attente afin de fournir la qualité de service demandée par un émetteur MSRP. La valeur représente le nombre maximal de trames que l'émetteur peut transmettre en une seconde.
VLAN de flux	ID VLAN du flux de trafic
MAC destination	Adresse MAC de la destination du flux de trafic
Réception de l'erreur de l'interface de pont d'informations	En cas de panne, interface du périphérique sur lequel la panne s'est produite
Code de défaillance des informations de panne reçues	Si une défaillance s'est produite, le numéro qui représente la raison de la défaillance. Le commutateur prend en charge les codes suivants : • 1 : Bande passante insuffisante • 3 : Bande passante insuffisante pour la classe de trafic • 5 : L'adresse de destination du flux est déjà utilisée • 7 : Latence signalée modifiée • 8 : Le port de sortie n'est pas compatible avec le pontage audio/vidéo (AVB) • 9 : Utilisez une adresse de destination différente (par exemple, si la table de hachage MAC DA est pleine) • 12 : Impossible de stocker l'adresse de destination (par exemple, si le périphérique n'a plus de ressources MAC DA) • 13 : La priorité demandée n'est pas une priorité de classe SR • 14 : MaxFrameSize est trop grand pour le support • 15 : la limite de msrpMaxFanInPorts a été atteinte • 16 : Modifications de FirstValue pour un StreamID enregistré • 17 : VLAN est bloqué sur ce port de sortie (enregistrement interdit)

Table 105 : Le PDSF diffuse des informations (A continué)

Champ	Description
Réception d'informations sur la panne MAC du pont	En cas de panne, adresse MAC du périphérique sur lequel la panne s'est produite
Interface de l'émetteur-récepteur	Interface sur laquelle l'émetteur est présent
Ecoute	Interface sur laquelle les auditeurs sont présents

Protection contre les boucles

La protection contre les boucles peut détecter les boucles physiques et logiques entre les ports Ethernet du commutateur.

Les boucles à l'intérieur d'un réseau peuvent être coûteuses car elles consomment des ressources et réduisent les performances du réseau. La détection manuelle des boucles peut s'avérer fastidieuse. Le commutateur peut identifier automatiquement les boucles dans le réseau. Vous pouvez activer la protection contre les boucles par port et globalement.

Si la protection contre les boucles est activée, le commutateur envoie des paquets PDU (Protocol Data Unit) prédéfinis à une adresse de destination de diffusion de couche 2 (FF :FF :FF :FF :FF :FF) sur tous les ports pour lesquels la fonction est activée. Vous pouvez désactiver de manière sélective la transmission de paquets PDU pour la protection contre les boucles sur des ports spécifiques, même lorsque la protection contre les boucles de port est activée. Si le commutateur reçoit un paquet avec l'adresse de destination de diffusion mentionnée précédemment, l'adresse MAC source dans le paquet est comparée à l'adresse MAC du commutateur. Si l'adresse MAC ne correspond pas, le paquet est transmis à tous les ports qui sont membres du même VLAN, comme tout autre paquet de diffusion. Le paquet n'est pas transmis au port à partir duquel informatique a été reçu

Si l'adresse MAC source correspond à l'adresse MAC du commutateur, le commutateur peut effectuer l'une des actions suivantes, selon la manière dont vous configurez l'action :

- Le port est désactivé.
- Un message de journal est généré. (Si un serveur syslog est configuré, le message de journal peut être envoyé au serveur syslog.)
- Le port est arrêté et un message de journal est généré.

La protection contre les boucles n'est pas destinée aux ports servant de liaisons montantes entre les commutateurs compatibles Spanning Tree. informatique est destiné aux switchs non manageables qui abandonnent les BPDU Spanning Tree. La protection contre les boucles détecte les boucles physiques et logiques entre les ports Ethernet

d'un périphérique. Vous devez activer la protection contre les boucles globalement avant de pouvoir activer et configurer informatique au niveau de l'interface. La protection contre les boucles est prise en charge sur les interfaces physiques et les interfaces lag statiques, mais pas sur les interfaces lag dynamiques.

À propos de la protection contre les boucles

Les boucles à l'intérieur d'un réseau sont coûteuses car elles consomment des ressources et réduisent les performances du réseau. La détection manuelle des boucles peut s'avérer fastidieuse.

Le commutateur peut identifier automatiquement les boucles dans le réseau. Vous pouvez activer la protection contre les boucles par port ou globalement.

Si la protection contre les boucles est activée, le commutateur envoie des paquets PDU (Protocol Data Unit) prédéfinis à une adresse de destination multicast de couche 2 (09 :00 :09 :09 :13 :A6) sur tous les ports pour lesquels la fonction est activée. Vous pouvez désactiver de manière sélective la transmission de paquets PDU pour la protection contre les boucles sur des ports spécifiques, même lorsque la protection contre les boucles de port est activée. Si le commutateur reçoit un paquet avec l'adresse de destination multicast mentionnée précédemment, l'adresse MAC source dans le paquet est comparée à l'adresse MAC du commutateur. Si l'adresse MAC ne correspond pas, le paquet est transmis à tous les ports membres du même VLAN, comme tout autre paquet multicast. Le paquet n'est pas transmis au port à partir duquel informatique a été reçu.

Si l'adresse MAC source correspond à l'adresse MAC du commutateur, le commutateur peut effectuer l'une des actions suivantes, selon la manière dont vous configurez l'action :

- Le port est désactivé.
- Un message de journal est généré. (Si un serveur syslog est configuré, le message de journal peut être envoyé au serveur syslog.)
- Le port est arrêté et un message de journal est généré.

Si la protection contre les boucles est désactivée, le paquet multicast est abandonné silencieusement.

La protection contre les boucles n'est pas destinée aux ports servant de liaisons montantes entre les commutateurs compatibles Spanning Tree. La protection contre les boucles est conçue pour les switches non manageables qui abandonnent les unités de données de protocole de pont (BPDU) Spanning Tree.

Vous devez activer la fonctionnalité globalement avant de pouvoir activer informatique au niveau du port afin que le filtre de stratégie système puisse être installé.

La protection contre les boucles traite la transmission des paquets PDU et le protocole Spanning Tree de la manière suivante :

- **Protection de boucle et transmission de paquets PDU** : La protection contre les boucles envoie des paquets de protocole de boucle à partir de tous les ports sur lesquels l'information est activée. Vous pouvez configurer l'intervalle (1 à 5 secondes) entre deux paquets PDU de protection de boucle successifs. L'intervalle par défaut est de 5 secondes. Si le commutateur reçoit un paquet de protocole de boucle sur un port pour lequel l'action est définie pour arrêter le port, le port ne peut plus recevoir et envoyer de trames.

La protection contre les boucles fonctionne au niveau du port, indépendamment de l'affectation et de l'appartenance de VLAN, détectant les boucles sur les VLAN.

- **Protocole Spanning Tree et protection contre les boucles** : La protection contre les boucles n'a pas d'impact sur les nœuds finaux et n'est pas destinée aux ports servant de liaisons montantes entre les commutateurs compatibles Spanning Tree. La protection contre les boucles peut coexister avec le protocole STP (Spanning Tree Protocol). Vous pouvez activer à la fois la protection contre les boucles et le protocole STP sur un port car ces fonctions fonctionnent indépendamment l'une de l'autre. Le protocole STP n'arrête pas un port lorsqu'une boucle est détectée, mais maintient le port en état de blocage. Comme les PDU sont autorisées dans un état de blocage, les paquets de protection de boucle sont reçus et la protection de boucle fait tomber le port impliqué dans la boucle (si l'action configurée est d'arrêter le port).

Configurez les paramètres globaux de protection contre les boucles

Avant de pouvoir configurer la protection contre les boucles pour des ports individuels (voir [Configurez les paramètres de protection contre les boucles pour les interfaces et affichez l'état de protection contre les boucles](#) à la page 523), vous devez activer et configurer globalement la protection contre les boucles.

Pour activer et configurer globalement la protection contre les boucles :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > L2 Loop protection > L2 Loop protection Configuration**.

La page L2 Loop protection Configuration s'affiche.

6. Dans la section Configuration de la protection contre les boucles L2 globale, configurez les paramètres suivants :
 - En regard de mode Admin, sélectionnez le bouton radio **Activer** ou **désactiver** pour spécifier le mode d'administration de la protection contre les boucles sur le commutateur.
Par défaut, la protection contre les boucles est globalement désactivée.
 - Dans le menu **intervalle annoncé TLV**, sélectionnez l'intervalle entre les transmissions de paquets en boucle sur un port.
La plage est de 1 à 5 secondes. La valeur par défaut est de 5 secondes. L'intervalle sélectionné s'applique à tous les ports pour lesquels vous activez la protection contre les boucles.
 - Dans le menu **Max PDU Receive**, sélectionnez le nombre maximal de paquets qu'un port peut recevoir avant qu'une action ne soit entreprise.
Le paramètre par défaut est 1 paquet. Le nombre de paquets sélectionné s'applique à tous les ports pour lesquels vous activez la protection contre les boucles.

7. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez les paramètres de protection contre les boucles pour les interfaces et affichez l'état de protection contre les boucles

Avant de pouvoir configurer la protection contre les boucles pour des ports individuels, vous devez activer globalement la protection contre les boucles (voir [Configurez les paramètres globaux de protection contre les boucles](#) à la page 521).

Pour activer et configurer la protection contre les boucles pour une interface et afficher l'état de protection contre les boucles sur le commutateur :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **commutation > L2 Loop protection > L2 Loop protection Configuration**.

La page L2 Loop protection Configuration s'affiche.

6. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :
 - **1 ou ID d'unité pour un commutateur empilé :**
 - 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
 - **ID d'unité pour un commutateur empilé :** Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
 - LAG Seuls les LAG sont affichés.
 - **Tous:** Les interfaces physiques et les LAG sont affichés, ou pour une pile de commutateurs, les interfaces physiques de tous les commutateurs de la pile et les LAG sont affichés.
7. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :
 - Pour afficher ou effacer les statistiques d'une seule interface, cochez la case associée à l'interface ou saisissez le numéro de l'interface dans le champ **aller à l'interface** et cliquez sur le bouton **aller**.
 - Pour configurer plusieurs interfaces avec les mêmes paramètres, cochez la case associée à chaque interface.
 - Pour configurer toutes les interfaces avec les mêmes paramètres, cochez la case dans la ligne d'en-tête.
8. Dans le menu **Keep Alive**, sélectionnez **Enable** pour spécifier que la protection contre les boucles doit être activée sur le port.

Par défaut, la protection contre les boucles est désactivée pour un port.
9. Dans le menu **action RX**, sélectionnez l'action que le commutateur effectue lorsqu'une boucle est détectée sur le port :
 - Journal Consignez le message lorsqu'une boucle est détectée sur le port.
 - Désactiver : Désactivez le port lorsqu'une boucle est détectée. Il s'agit de l'option par défaut.
 - **Les deux:** Consigner et désactiver le port lorsqu'une boucle est détectée.
10. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.
11. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.
12. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

Le tableau suivant décrit les champs en lecture seule de la page.

Table 106 : Informations de configuration de l'interface de protection contre les boucles

Champ	Description
Détection de boucle	Indique (Oui ou non) si une boucle est détectée sur l'interface
Nombre de boucles	Nombre de paquets reçus sur l'interface après la détection de la boucle
Temps écoulé depuis la dernière boucle	Temps écoulé depuis la détection de la boucle
Etat du port	État de l'interface (activé ou Désactivé)
Motif de désactivation de l'erreur	Raison pour laquelle l'interface a été désactivée. En plus d'être désactivée en raison de la protection contre les boucles, l'interface peut être désactivée en raison de la détection de liaison unidirectionnelle (UDLD), d'une tempête de diffusion, d'une tempête de monodiffusion, etc.
Temps de récupération automatique restant (s)	Temps restant avant que l'interface ne soit réactivée via le processus de récupération automatique. La durée est comprise entre 30 et 604800 secondes.

5

Gérer le routage

Ce chapitre aborde les sujets suivants :

- Concepts de routage
- Table de routage, routes et préférences de route
- Routage IPv4
- Routage IPv6
- VLAN de routage
- Protocole de résolution d'adresse
- Protocole d'informations de routage
- Découverte de routeurs et annonces de routeurs
- Virtual Router Redundancy Protocol

Concepts de routage

Le commutateur prend en charge le routage IP. Lorsqu'un paquet entre dans le commutateur, celui-ci vérifie l'adresse MAC de destination pour déterminer si informatique correspond à l'une des interfaces de routage configurées. Si informatique le fait, le commutateur recherche une adresse IP de destination correspondante dans la table des hôtes. Si une entrée correspondante est trouvée, le paquet est acheminé vers l'hôte. Si aucune entrée correspondante n'est trouvée, le commutateur effectue une correspondance de préfixe la plus longue sur l'adresse IP de destination. Si une entrée correspondante est trouvée, le paquet est acheminé vers le saut suivant. Si aucune entrée correspondante n'est trouvée, le paquet est acheminé vers le saut suivant spécifié dans la route par défaut. Si aucune route par défaut n'existe, le paquet est abandonné.

Table de routage, routes et préférences de route

La table de routage collecte les routes provenant de plusieurs sources et répertorie toutes les routes : routes statiques, routes locales, routes ajoutées dynamiquement, etc. Les routes statiques sont des routes que vous ajoutez manuellement. La table de routage peut apprendre plusieurs routes vers la même destination à partir de plusieurs sources, par exemple des routes ajoutées dynamiquement via des protocoles de routage.

Configurer une route et afficher les routes apprises

Vous pouvez ajouter ou modifier une route dans la table de routage et afficher les routes automatiquement apprises dans la table de routage.

Pour ajouter ou modifier un itinéraire et afficher les itinéraires appris :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > table de routage > basique > Configuration de routage**.

La page Configuration de la route s'affiche.

6. Si vous modifiez un itinéraire existant, cochez la case de l'itinéraire.
7. Dans le menu **type d'itinéraire**, sélectionnez l'un des types d'itinéraire suivants :
 - Par défaut Spécifiez l'adresse et la préférence du saut suivant.
 - Statique Spécifiez l'adresse réseau, le masque de sous-réseau, l'adresse du saut suivant et la préférence.
 - **Rejet statique** : Spécifiez l'adresse réseau, le masque de sous-réseau et la préférence.
8. Dans le champ **adresse réseau**, entrez le préfixe de route IP de la destination.
9. Dans le champ **masque de sous-réseau**, entrez la partie de l'adresse de l'interface IP qui identifie le réseau connecté.
Il est également appelé masque de sous-réseau/réseau.
10. Dans le champ **adresse IP du saut suivant**, entrez l'adresse IP du routeur sortant qui doit être utilisée lorsque le trafic est transféré au routeur suivant (le cas échéant) dans le chemin vers la destination.

Le routeur suivant est toujours l'un des voisins adjacents ou l'adresse IP de l'interface locale pour un réseau directement connecté.

11. Dans le champ **taille MTU**, entrez une valeur comprise entre 1 et 255.

Vous pouvez spécifier la valeur de préférence (parfois appelée distance administrative) d'une route statique individuelle. Parmi les routes vers la même destination, la route ayant la valeur de préférence la plus faible est la route entrée dans la base de données de transfert. En spécifiant la préférence d'une route statique, vous pouvez contrôler si une route statique est plus préférée ou moins préférée que les routes issues de protocoles de routage dynamiques. La préférence détermine également si une route statique est plus préférée ou moins préférée que d'autres routes statiques vers la même destination.

12. Dans le champ **Description**, entrez la description de cette route qui identifie la route.

La description doit être composée de caractères alphanumériques, de tirets ou de traits de soulignement et peut contenir jusqu'à 31 caractères.

13. Effectuez l'une des opérations suivantes :

- Si vous ajoutez une nouvelle route, cliquez sur le bouton **Ajouter**.
Les paramètres sont enregistrés. La route est ajoutée à la table de routage.
- Si vous modifiez un itinéraire existant, cliquez sur le bouton **appliquer**.
Les paramètres sont enregistrés.

14. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 107 : Informations sur les routes apprises

Champ	Description
Adresse réseau	Préfixe de route IP pour la destination.
Masque de sous-réseau	Masque de sous-réseau/réseau, qui indique la partie de l'adresse de l'interface IP qui identifie le réseau connecté.
Protocole	Protocole qui a créé la route : Local, statique, OSPF ou RIP.
Type de route	Le type de route, en fonction du protocole : Connecté, statique ou dynamique.
Interface de saut suivant	Interface de l'interface du routeur sortant qui doit être utilisée lorsque le trafic est transféré vers la destination.
Adresse du saut suivant	Adresse IP de l'interface du routeur sortant qui doit être utilisée lorsque le trafic est transféré au routeur suivant (le cas échéant) dans le chemin vers la destination.
Préférences	La préférence, qui est une valeur comprise entre 0 et 255.
Métrique	Coût administratif du chemin vers la destination. Le numéro par défaut est 1. La plage est de 0 à 255.

Supprimer un itinéraire

Vous pouvez supprimer un itinéraire dont vous n'avez plus besoin.

Pour supprimer un itinéraire :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > table de routage > basique > Configuration de routage**.

La page Configuration de la route s'affiche.

6. Cochez les cases correspondant au contenu.

7. Cliquez sur le bouton **Supprimer**.

Les paramètres sont enregistrés. La route est supprimée.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Spécifiez les préférences d'itinéraire

Vous pouvez configurer la préférence par défaut pour chaque protocole, par exemple, 60 pour les routes statiques ou 120 pour le protocole RIP. Ces valeurs sont des valeurs arbitraires comprises entre 1 et 255 et sont indépendantes des métriques de route. La plupart des protocoles de routage utilisent une métrique de route pour déterminer le chemin le plus court connu du protocole, indépendamment de tout autre protocole.

Le meilleur itinéraire vers une destination est choisi en sélectionnant l'itinéraire avec la valeur de préférence la plus basse. S'il existe plusieurs routes vers une destination, les valeurs de préférence sont utilisées pour déterminer la route préférée. S'il y a toujours égalité, la route avec la meilleure métrique de route est choisie. Pour éviter les problèmes liés à des mesures non concordantes, telles que des protocoles qui ne sont pas directement comparables, vous devez configurer des valeurs de préférence différentes pour chacun des protocoles.

Pour spécifier les préférences d'itinéraire

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > table de routage > Avancé > Préférences d'itinéraire** .

La page Préférences d'itinéraire s'affiche.

6. Dans le champ **statique**, spécifiez la préférence de route statique sur le commutateur.
La valeur par défaut est 1. La plage est de 1 à 255.
7. Dans le champ **RIP**, spécifiez la préférence de route RIP sur le commutateur.
La valeur par défaut est 120. La plage est de 1 à 255.
8. Dans le champ **OSPF intra**, spécifiez la préférence de route OSPF intra sur le commutateur.
La valeur par défaut est 110. La plage est de 1 à 255.
9. Dans le champ **Inter OSPF**, spécifiez la préférence inter route OSPF sur le commutateur.
La valeur par défaut est 110. La plage est de 1 à 255.
10. Dans le champ **externe OSPF**, spécifiez la préférence de route externe OSPF sur le commutateur.
La valeur par défaut est 110. La plage est de 1 à 255.
11. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
Le champ local affiche la valeur de préférence d'itinéraire local.
12. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Routage IPv4

Vous pouvez activer ou désactiver le mode de routage IPv4, configurer les paramètres de routage IPv4 globaux, configurer les interfaces de routage IPv4, ajouter une adresse IP secondaire à une interface de routage IPv4 et afficher les statistiques de routage IPv4.

Gérer les paramètres de routage IPv4 globaux

Vous pouvez configurer les paramètres de routage IPv4 du commutateur, par opposition aux paramètres de routage IPv4 d'une interface.

Pour configurer les paramètres de routage IPv4 globaux :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > IP > basique > Configuration IP**.

L'écran IP Configuration (Configuration IP) s'affiche.

6. Sélectionnez le bouton radio **Activer** ou **désactiver** le mode de routage.

Cette sélection active ou désactive le mode administratif pour le routage IPv4 pour le commutateur. La valeur par défaut est Activer.

7. Sélectionnez le bouton radio **Activer** ou **désactiver** les réponses d'écho ICMP.

La valeur par défaut est enable, ce qui signifie que le commutateur envoie des réponses d'écho ICMP aux demandes d'écho ICMP.

8. Sélectionnez le bouton radio **Activer** ou **désactiver** les redirections ICMP.

La valeur par défaut est désactiver. Si vous activez les redirections ICMP, le commutateur peut transférer les redirections ICMP.

9. Dans le champ **intervalle de limite de débit ICMP**, spécifiez le nombre de paquets d'erreur ICMP autorisés par intervalle de rafale.

Par défaut, l'intervalle de rafale est de 1000 ms (la limite de débit est de 100 paquets/sec). L'intervalle est compris entre 0 et 2147483647 ms. Entrez 0 pour laisser le commutateur ignorer le nombre de paquets d'erreur ICMP autorisés par intervalle de rafale.

10. Dans le champ **ICMP Rate Limit Burst Size**, spécifiez le nombre de paquets d'erreur ICMP autorisés pour la taille de rafale.

Par défaut, la taille des rafales est de 100 paquets. La plage de taille de rafale est comprise entre 1 et 200. Entrez 0 pour laisser le commutateur ignorer le nombre de paquets d'erreur ICMP autorisés pour la taille de rafale.

11. Pour configurer une passerelle globale par défaut, cochez la case **sélectionner pour configurer la passerelle globale par défaut**. Ensuite, dans le champ **passerelle par défaut globale**, entrez l'adresse IP.

La passerelle par défaut que vous spécifiez reçoit une préférence plus élevée qu'une passerelle par défaut apprise à partir d'un serveur DHCP. Vous configurez une seule passerelle par défaut, mais vous pouvez modifier la passerelle par défaut.

12. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

13. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 108 : Informations de configuration du routage IPv4

Champ	Description
Durée de vie par défaut	Valeur par défaut insérée dans le champ Time-To-Live de l'en-tête IP des datagrammes émis par le commutateur, si une valeur TTL n'est pas fournie par le protocole de couche transport.
Sauts suivants maximum	Nombre maximal de sauts pris en charge par le commutateur.
Nombre maximal d'itinéraires	Nombre maximal de routes prises en charge par le commutateur.
Routes statiques maximales	Nombre maximal de routes statiques prises en charge par le commutateur.

Afficher les statistiques IPv4

Vous pouvez afficher les statistiques de routage IPv4 pour le commutateur.

Pour afficher les statistiques de routage IPv4 pour le commutateur :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > IP > basique > statistiques**.

La page statistiques s'affiche.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 109 : Informations statistiques IP

Champ	Description
IpInReceives	Nombre total de datagrammes d'entrée reçus des interfaces, y compris ceux reçus par erreur.
Erreurs IpInHdrErrors	Le nombre de datagrammes d'entrée rejetés en raison d'erreurs dans leurs en-têtes IP, y compris les sommes de contrôle erronées, la non-correspondance de numéro de version, d'autres erreurs de format, le délai de vie dépassé, les erreurs découvertes dans le traitement de leurs options IP, etc.
IpInAddrErrors	Nombre de datagrammes d'entrée ignorés car l'adresse IP dans le champ de destination de leur en-tête IP n'était pas une adresse valide à recevoir sur cette entité. Ce nombre inclut les adresses non valides (par exemple, 0,0,0,0) et les adresses de classes non prises en charge (classe E). Pour les entités qui ne sont pas des passerelles IP et qui ne transmettent donc pas de datagrammes, ce compteur inclut les datagrammes rejetés car l'adresse de destination n'était pas une adresse locale.
IpForwDatagrammes	Le nombre de datagrammes d'entrée pour lesquels cette entité n'était pas leur destination IP finale, à la suite de quoi une tentative a été faite pour trouver une route pour les transférer à cette destination finale. Dans les entités qui n'agissent pas en tant que passerelles IP, ce compteur inclut uniquement les paquets qui ont été acheminés à la source via cette entité, et le traitement de l'option source-route a réussi.

Table 109 : Informations statistiques IP (A continué)

Champ	Description
IpInUnknownProtos	Nombre de datagrammes adressés localement reçus avec succès mais rejetés en raison d'un protocole inconnu ou non pris en charge.
IpInDiscards	Nombre de datagrammes IP d'entrée pour lesquels aucun problème n'a été rencontré pour empêcher leur traitement continu, mais qui ont été rejetés (manque d'espace tampon). Ce compteur n'inclut pas les datagrammes rejetés en attente de réassemblage.
IpInDelivers	Nombre total de datagrammes d'entrée livrés avec succès aux protocoles utilisateur IP (y compris ICMP).
IpOutRequests	Nombre total de datagrammes IP que les protocoles utilisateur IP locaux (y compris ICMP) ont fournis à IP dans les demandes de transmission. Ce compteur n'inclut pas les datagrammes comptés dans ipForwDatagrammes.
IpOutDiscards	Nombre de datagrammes IP de sortie pour lesquels aucun problème n'a été rencontré pour empêcher leur transmission à leur destination, mais qui ont été rejetés pour des raisons telles que le manque d'espace tampon. Ce compteur inclurait les datagrammes comptés dans ipForwDatagrammes si de tels paquets remplissaient ce critère de rejet (discrétionnaire).
IpOutNoRoutes	Nombre de datagrammes IP rejetés car aucune route n'a pu être trouvée pour les transmettre à leur destination. Ce compteur inclut tous les paquets comptés dans ipForwDatagrammes qui répondent à ce critère de non-route. Cela inclut tous les datagrammes qu'un hôte ne peut pas acheminer parce que toutes ses passerelles par défaut sont hors service.
Expiration IpReasmTimeout	Nombre maximal de secondes pendant lesquelles les fragments reçus sont conservés pendant qu'ils sont en attente de réassemblage au niveau de cette entité.
IpReasmReqds	Nombre de fragments IP reçus qui ont été réassemblés au niveau de cette entité.
IpReasmOKs	Nombre de datagrammes IP réassemblés avec succès.
IpReasmFails	Nombre d'échecs détectés par l'algorithme de réassemblage IP (pour une raison quelconque : expiration du délai, erreurs, etc.). Il ne s'agit pas nécessairement d'un nombre de fragments IP rejetés puisque certains algorithmes peuvent perdre la trace du nombre de fragments en les combinant au fur et à mesure qu'ils sont reçus.
IpFragOKs	Nombre de datagrammes IP fragmentés au niveau de cette entité.
IpFragFails	Le nombre de datagrammes IP qui ont été rejetés parce qu'ils devaient être fragmentés au niveau de cette entité, mais ne pouvaient pas l'être, pour des raisons telles que leur drapeau ne pas fragmenter a été défini.
IpFragCreates	Nombre de fragments de datagramme IP générés à la suite de la fragmentation au niveau de cette entité.

Table 109 : Informations statistiques IP (A continué)

Champ	Description
IpRoutingDiscards	Nombre d'entrées de routage qui ont été supprimées alors qu'elles étaient valides. Une raison possible pour rejeter une telle entrée pourrait être de libérer de l'espace tampon pour d'autres entrées de routage.
IcmpInMsgs	Nombre total de messages ICMP reçus par l'entité. Ce compteur inclut tous ceux comptés par icmpInErrors.
IcmpInErrors	Nombre de messages ICMP reçus par l'entité mais identifiés comme présentant des erreurs spécifiques à ICMP (sommes de contrôle ICMP erronées, longueur incorrecte, etc.).
IcmpInDestUnreachs	Nombre de messages de destination ICMP inaccessibles reçus.
IcmpInTimeExcds	Le nombre de messages reçus ayant dépassé le délai ICMP.
IcmpInParmProbs	Nombre de messages de problème de paramètre ICMP reçus.
IcmpInSrcQuenchs	Nombre de messages d'extinction de source ICMP reçus.
IcmpInRedirects	Nombre de messages de redirection ICMP reçus.
IcmpInEchos	Nombre de messages d'écho ICMP (requête) reçus.
IcmpInEchoReps	Nombre de messages de réponse d'écho ICMP reçus.
IcmpInTimestamps	Nombre de messages d'horodatage ICMP (requête) reçus.
IcmpInTimestampReps	Nombre de messages de réponse d'horodatage ICMP reçus.
IcmpInAddrMasks	Nombre de messages de demande de masque d'adresse ICMP reçus.
IcmpInAddrMaskReps	Nombre de messages de réponse de masque d'adresse ICMP reçus.
IcmpOutMsgs	Nombre total de messages ICMP que cette entité a tenté d'envoyer. Ce compteur inclut tous ceux comptés par icmpOutErrors.
IcmpOutErrors	Nombre de messages ICMP que cette entité n'a pas envoyés en raison de problèmes découverts dans ICMP, tels qu'un manque de tampons. Cette valeur n'inclut pas les erreurs découvertes en dehors de la couche ICMP, telles que l'incapacité d'IP à acheminer le datagramme résultant. Dans certaines implémentations, il peut n'y avoir aucun type d'erreur qui contribue à la valeur de ce compteur.
IcmpOutDestUnreachs	Nombre de messages de destination ICMP inaccessibles envoyés.
IcmpOutTimeExcds	Le nombre de messages ICMP dépassés envoyés.
IcmpOutParmProbs	Nombre de messages de problème de paramètre ICMP envoyés.
IcmpOutSrcQuenchs	Nombre de messages de quench source ICMP envoyés.
IcmpOutRedirects	Nombre de messages de redirection ICMP envoyés. Pour un hôte, cette valeur est toujours égale à zéro, car les hôtes n'envoient pas de redirections.
IcmpOutEchos	Nombre de messages d'écho ICMP (requête) envoyés.

Table 109 : Informations statistiques IP (A continué)

Champ	Description
IcmpOutEchoReps	Nombre de messages de réponse d'écho ICMP envoyés.
IcmpOutTimestamps	Le nombre de messages d'horodatage ICMP (requête).
IcmpOutTimestampReps	Nombre de messages de réponse d'horodatage ICMP envoyés.
IcmpOutAddrMasks	Nombre de messages de demande de masque d'adresse ICMP envoyés.

Configurer les interfaces de routage IPv4

Vous pouvez configurer une ou plusieurs interfaces de routage IPv4.

Pour configurer une ou plusieurs interfaces de routage IPv4 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > IP > Avancé > Configuration de l'interface IP**.

L'écran IP Configuration (Configuration IP) s'affiche.

6. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :
 - **1 ou ID d'unité pour un commutateur empilé :**
 - 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
 - **ID d'unité pour un commutateur empilé :** Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
 - VLAN Seuls les VLAN sont affichés.
 - **Tous:** Les interfaces physiques et les VLAN sont affichés, ou pour une pile de commutateurs, les interfaces physiques et les VLAN de tous les commutateurs sont affichés.
 7. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :
 - Pour afficher ou effacer les statistiques d'une seule interface, cochez la case associée à l'interface ou saisissez le numéro de l'interface dans le champ **aller à l'interface** et cliquez sur le bouton **aller**.
 - Pour configurer plusieurs interfaces avec les mêmes paramètres, cochez la case associée à chaque interface.
 - Pour configurer toutes les interfaces avec les mêmes paramètres, cochez la case dans la ligne d'en-tête.
 8. Dans le champ **Description**, entrez une description de l'interface.
 9. Dans le menu **IP Address Configuration Method**, sélectionnez la méthode de configuration d'une adresse IP sur l'interface : **Aucun**, **Manuel** ou **DHCP**.

Par défaut, la méthode est None. Utilisez la méthode aucun pour réinitialiser la méthode DHCP.

❗ Remarque: Lorsque vous modifiez la méthode de configuration de DHCP à aucun, un délai mineur se produit avant que la page ne soit actualisée.
 10. Si vous sélectionnez **Manuel** dans le menu **méthode de configuration de l'adresse IP**, procédez comme suit :
 - a. Dans le champ **adresse IP**, entrez l'adresse IP de l'interface.
 - b. Dans le champ **masque de sous-réseau**, entrez le masque de sous-réseau de l'interface.

Il est également appelé masque de sous-réseau/réseau et définit la partie de l'adresse IP de l'interface utilisée pour identifier le réseau connecté.
 11. Dans le menu **mode de routage**, sélectionnez **Activer** ou **désactiver** pour activer ou désactiver le mode de routage de l'interface.
-

La valeur par défaut est Activer.

12. Dans le menu **mode administratif**, sélectionnez **Activer** ou **désactiver** pour activer ou désactiver le mode administratif de l'interface.

La valeur par défaut est Activer.

13. Dans le menu **transférer les diffusions dirigées sur le réseau**, sélectionnez **Activer** ou **désactiver** pour activer ou désactiver le transfert des paquets de diffusion dirigés sur le réseau.

La valeur par défaut est Disable, ce qui signifie que les paquets de diffusion dirigés vers le réseau ne sont pas transférés mais abandonnés.

14. Dans le menu **type d'encapsulation**, sélectionnez le type d'encapsulation de la couche liaison pour les paquets transmis à partir de l'interface spécifiée.

Vous pouvez sélectionner **Ethernet** ou **SNAP**, qui est le protocole d'accès au sous-réseau. La valeur par défaut est Ethernet.

15. Dans le menu **Proxy Arp**, sélectionnez **Activer** ou **désactiver** pour activer ou désactiver le proxy ARP pour l'interface.

La valeur par défaut est Activer.

16. Dans le menu **local Proxy Arp**, sélectionnez **Activer** ou **désactiver** pour activer ou désactiver le proxy local ARP pour l'interface.

La valeur par défaut est désactiver.

17. Dans le champ **Bandwidth (kbps) (bande passante (kbps))**, spécifiez la bande passante de l'interface.

Ces informations dans ce champ déterminent la vitesse de l'interface vers les protocoles de niveau supérieur. Certains protocoles utilisent la bande passante pour calculer le coût de la liaison. La plage est de 1 à 10000000.

18. Dans le menu **ICMP destination Unreachables**, sélectionnez **Enable** ou **Disable** pour activer ou désactiver l'envoi par l'interface de messages ICMP destination unreachable.

La valeur par défaut est Activer.

19. Dans le menu **redirections ICMP**, sélectionnez **Activer** ou **désactiver** pour activer ou désactiver le mode de redirection ICMP.

L'interface envoie un message de redirection ICMP uniquement si cette fonction est activée à la fois globalement et sur l'interface. La valeur par défaut est Activer.

20. Dans le champ **IP MTU**, spécifiez la taille maximale des paquets IP envoyés sur l'interface.

La MTU IP correspond à la taille de trame maximale moins la longueur de l'en-tête de couche 2. La plage va de 68 octets à la taille MTU prise en charge par la liaison d'interface. Le numéro par défaut est 1500. La valeur 0 indique que la MTU IP n'est

pas configurée, auquel cas l'interface utilise la taille de MTU prise en charge par la liaison d'interface.

21. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

22. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 110 : Interfaces IP (configurables)

Champ	Description
Identifiant VLAN	ID VLAN de l'interface
Débit de données de la vitesse de liaison	Débit de données de la liaison physique de l'interface
Mode Admin OSPF	Indique si OSPF est activé (Activer) ou désactivé (désactiver) pour l'interface
État actif	État actif ou inactif de l'interface (actif ou Inactif)
Adresse MAC	Adresse MAC associée à l'interface
Etat du lien	État de liaison active ou inactive de l'interface. (Liaison ascendante ou liaison descendante.) Une interface est considérée comme active si la liaison est active et que l'interface est en état de transfert. Interface configurée pour l'empilement à l'état détaché (détaché).
État de l'interface de routage	État de liaison de l'interface de routage (up ou down)

Supprimez l'adresse IP de routage d'une interface de routage IPv4

Vous pouvez supprimer l'adresse IP de routage d'une ou plusieurs interfaces de routage IPv4.

Pour supprimer l'adresse IP de routage d'une ou plusieurs interfaces de routage IPv4 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > IP > Avancé > Configuration de l'interface IP**.

L'écran IP Configuration (Configuration IP) s'affiche.

6. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :

- **1 ou ID d'unité pour un commutateur empilé :**
 - 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
 - **ID d'unité pour un commutateur empilé :** Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
- **VLAN** Seuls les VLAN sont affichés.
- **Tous:** Les interfaces physiques et les VLAN sont affichés, ou pour une pile de commutateurs, les interfaces physiques et les VLAN de tous les commutateurs sont affichés.

7. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :

- Pour afficher ou effacer les statistiques d'une seule interface, cochez la case associée à l'interface ou saisissez le numéro de l'interface dans le champ **aller à l'interface** et cliquez sur le bouton **aller**.
- Pour effacer les statistiques de plusieurs interfaces, cochez la case associée à chaque interface.

8. Cliquez sur le bouton **Supprimer**.

Les paramètres sont enregistrés. L'adresse de routage IP est supprimée de l'interface de routage IPv4.

9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez une adresse IP secondaire pour une interface de routage IPv4

Vous pouvez configurer une adresse IP secondaire pour une interface de routage IPv4.

Pour configurer l'adresse IP secondaire :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > IP > Avancé > IP secondaire** .

La page adresse IP secondaire s'affiche.

6. Dans le menu **interface**, sélectionnez l'interface.

7. Dans le champ **adresse IP secondaire**, ajoutez une adresse IPv4 secondaire à l'interface.
8. Dans le champ **masque de sous-réseau IP secondaire**, entrez le masque de sous-réseau associé à l'adresse IP secondaire.
9. Cliquez sur le bouton **Add** (Ajouter).
L'adresse IP secondaire est ajoutée.
10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 111 : Informations sur l'adresse IP secondaire

Champ	Description
Identifiant VLAN	ID VLAN associé à l'interface sélectionnée.
Adresse IP principale	Adresse IP principale de l'interface.

Supprimez l'adresse IP secondaire d'une interface de routage IPv4

Vous pouvez supprimer l'adresse IP secondaire d'une interface de routage IPv4.

Pour supprimer l'adresse IP secondaire d'une interface de routage IPv4 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **roulage > IP > Avancé > IP secondaire**.

La page adresse IP secondaire s'affiche.

6. Dans le menu **interface**, sélectionnez l'interface.

7. Dans le tableau adresse IP secondaire, cochez la case correspondant à l'adresse IP.

8. Cliquez sur le bouton **Supprimer**.

Les paramètres sont enregistrés. L'adresse de routage IP secondaire est supprimée de l'interface de routage IPv4.

9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Routage IPv6

Vous pouvez activer ou désactiver le mode de routage IPv6, configurer les paramètres de routage IPv6 globaux, configurer les interfaces de routage IPv6, ajouter des préfixes IPv6, ajouter des routes statiques IPv6 et des préférences de route, ajouter des tunnels IPv6 et afficher les statistiques de routage IPv6, les routes et les voisins.

Gérer les paramètres de routage IPv6 globaux

Vous pouvez configurer les paramètres de routage IPv6 du commutateur, par opposition aux paramètres de routage IPv6 d'une interface.

Pour configurer les paramètres de routage IPv6 globaux :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > IPv6 > basique > Configuration globale**.

La page Configuration globale s'affiche.

6. Sélectionnez le bouton radio **Activer** ou **désactiver** le routage monodiffusion IPv6.

Cette sélection active ou désactive le mode administratif pour le routage IPv6 pour le commutateur. La valeur par défaut est désactiver.

7. Dans le champ **Hop Limit**, entrez une valeur pour le nombre de sauts de monodiffusion utilisé pour les paquets IPv6 provenant du commutateur.

Le nombre de sauts est également inclus dans les annonces du routeur et varie de 1 à 255 inclus. Le numéro par défaut est 64.

8. Dans le champ **intervalle d'erreur de limite de débit ICMPv6**, spécifiez le nombre de paquets d'erreur ICMP autorisés par intervalle de rafale.

Par défaut, l'intervalle de rafale est de 1000 ms (la limite de débit est de 100 paquets/sec). L'intervalle est compris entre 0 et 2147483647 ms. Entrez 0 pour laisser

le commutateur ignorer le nombre de paquets d'erreur ICMPv6 autorisés par intervalle de rafale.

9. Dans le champ **taille de salve de limite de débit ICMPv6**, spécifiez le nombre de paquets d'erreur ICMP autorisés pour la taille de salve.

Par défaut, la taille des rafales est de 100 paquets. La plage de taille de rafale est comprise entre 1 et 200. Entrez 0 pour laisser le commutateur ignorer le nombre de paquets d'erreur ICMPv6 autorisés pour la taille de rafale.

10. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

11. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Affichez la table de routage IPv6

La table de routage IPv6 inclut toutes les routes, y compris les meilleures routes et les routes configurées. Vous pouvez sélectionner les itinéraires à afficher.

Pour afficher la table de routage IPv6 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **routage > IPv6 > basique > table de routage** .
La page table de routage s'affiche.
6. Dans le menu **routes affichées**, sélectionnez les routes à afficher dans le tableau :
 - **Toutes les routes** : Toutes les routes IPv6 actives.
 - **Meilleurs itinéraires seulement** : Les meilleurs itinéraires actifs uniquement,
 - **Routes configurées uniquement** : Les routes configurées manuellement uniquement.
7. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).
Le tableau suivant décrit les champs en lecture seule de la page.

Table 112 : Informations sur la table de routage IPv6

Champ	Description
Nombre de routes	Nombre total de routes actives dans la table de routes.
Préfixe IPv6	Préfixe réseau de la route active.
Longueur de préfixe	Longueur du préfixe pour la route active.
Protocole	Type de protocole pour la route active.
Interface de saut suivant	Interface sur laquelle la route est active. Pour une route de rejet, le saut suivant est une interface nulle (Null0).
Adresse IP du saut suivant	Adresse IPv6 du tronçon suivant pour la route active.
Préférences	Préférence de route de la route configurée.

Configurer les interfaces de routage IPv6

Vous pouvez configurer une ou plusieurs interfaces de routage IPv6.

Pour configurer une ou plusieurs interfaces de routage IPv6 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > IPv6 > Avancé > statistiques d'interface** .

La page Configuration de l'interface s'affiche.

6. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :

- **1 ou ID d'unité pour un commutateur empilé :**
 - 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
 - **ID d'unité pour un commutateur empilé :** Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
- **VLAN** Seuls les VLAN sont affichés.
- **Tous:** Les interfaces physiques et les VLAN sont affichés, ou pour une pile de commutateurs, les interfaces physiques et les VLAN de tous les commutateurs sont affichés.

7. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :

- Pour afficher ou effacer les statistiques d'une seule interface, cochez la case associée à l'interface ou saisissez le numéro de l'interface dans le champ **aller à l'interface** et cliquez sur le bouton **aller**.
- Pour configurer plusieurs interfaces avec les mêmes paramètres, cochez la case associée à chaque interface.
- Pour configurer toutes les interfaces avec les mêmes paramètres, cochez la case dans la ligne d'en-tête.

8. Dans le menu **mode IPv6**, sélectionnez **Activer** ou **désactiver** pour activer ou désactiver le mode de routage IPv6 pour l'interface.
Lorsque le mode de routage IPv6 est activé, l'interface peut fonctionner avec IPv6 sans adresse globale. Dans ce cas, une adresse lien-local basée sur EUI-64 est utilisée. La valeur par défaut est désactiver.
9. Dans le menu **mode client DHCPv6**, sélectionnez **Activer** ou **désactiver** pour activer ou désactiver le mode client DHCPv6 sur l'interface.
Une seule interface peut fonctionner comme client DHCPv6. La valeur par défaut est désactiver.
10. Dans le menu **Stateless Address AutoConfig mode**, sélectionnez **Activer** ou **désactiver** pour activer ou désactiver le mode de configuration automatique d'adresse stateless sur l'interface.
La valeur par défaut est désactiver.
11. Dans le menu **mode de routage**, sélectionnez **Activer** ou **désactiver** pour activer ou désactiver le mode de routage de l'interface.
La valeur par défaut est désactiver.
12. Dans la liste **mode administrateur**, sélectionnez **Activer** ou **désactiver** pour activer ou désactiver le mode administratif de l'interface.
La valeur par défaut est Activer.
13. Dans le champ **MTU**, spécifiez l'unité de transmission maximale pour l'interface.
La plage est de 1280 à 1500. Le numéro par défaut est 1500. Si vous entrez 0, vous désactivez le routage sur l'interface.
14. Dans le champ **Duplicate Address Detection Transmissions (détection d'adresse en double)**, spécifiez le nombre de transmissions DAD (détection d'adresse en double) pour l'interface.
La valeur de transmission DAD doit être comprise entre 0 et 600. Le numéro par défaut est 1.
15. Dans le champ **intervalle de durée de vie**, spécifiez l'intervalle de durée de vie que l'interface transmet dans les annonces de routeur.
Il s'agit des informations sur la période pendant laquelle les voisins IPv6 peuvent utiliser l'interface comme routeur par défaut.
La plage est de 0 à 9000. Le numéro par défaut est 1800. La valeur doit être supérieure ou égale à l'intervalle d'annonce maximum. Si vous entrez 0, l'interface ne peut pas être utilisée comme interface de routage par défaut.
16. Dans le champ **Adv NS Interval**, spécifiez les informations sur l'intervalle de retransmission que l'interface transmet dans les annonces de routeur.
Il s'agit de l'information sur l'intervalle entre les retransmissions de sollicitation de voisins.

La plage est de 1000 à 4294967295. Le numéro par défaut est 0.

17. Dans le champ **Adv Rejoignable Interval**, spécifiez les informations d'intervalle d'accessibilité que l'interface transmet dans les annonces de routeur.

Il s'agit des informations sur la période pendant laquelle un périphérique IPv6 distant est considéré comme accessible après réception d'un message de confirmation de découverte de voisin.

La plage est de 0 à 3600000. Le numéro par défaut est 0.

18. Dans le champ **intervalle avancé**, spécifiez la période entre les annonces de routeur à partir de l'interface.

La plage est de 4 à 1800. Le numéro par défaut est 600.

19. Dans le menu **indicateur de configuration Adv Management**, sélectionnez **Activer** ou **désactiver** pour activer ou désactiver l'annonce de routeur « indicateur de configuration d'adresse gérée » pour l'interface.

Lorsque cette option est activée, les nœuds finaux utilisent DHCPv6. Lorsque cette option est désactivée, les nœuds finaux configurent automatiquement les adresses. La valeur par défaut est désactiver.

20. Dans le menu **Adv Other Config Flag**, sélectionnez **Enable** ou **Disable** pour activer ou désactiver l'annonce du routeur « Other stateful configuration flag » pour l'interface.

La valeur par défaut est désactiver. L'autre indicateur de configuration avec état indique à un hôte IPv6 d'utiliser DHCPv6 pour obtenir des informations de configuration supplémentaires telles que, par exemple, l'adresse IPv6 d'un serveur DNS.

21. Dans le menu **Préférences du routeur**, sélectionnez les annonces de préférences du routeur pour l'interface.

Vous pouvez sélectionner **Haut**, **moyen** ou **Bas**. La valeur par défaut est moyenne.

22. Dans la liste **drapeau de suppression avancée**, sélectionnez **Activer** ou **désactiver** pour activer ou désactiver la suppression de la publicité du routeur pour l'interface.

La valeur par défaut est désactiver.

23. Dans le menu **destination inaccessible**, sélectionnez **Activer** ou **désactiver** pour activer ou désactiver la transmission du message ICMPv6 destination inaccessible sur l'interface.

La valeur par défaut est Activer.

24. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

25. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 113 : Informations de configuration de l'interface IPv6

Champ	Description
Mode de fonctionnement	État opérationnel d'une interface. La valeur par défaut est désactiver.
Etat du lien	Indique si la liaison est active ou inactive (liaison active ou liaison inactive).

Configurer les paramètres de préfixe pour une interface de routage IPv6

Vous pouvez ajouter ou modifier un ou plusieurs préfixes et paramètres associés pour une interface de routage IPv6.

Pour ajouter ou modifier les paramètres de préfixe d'une interface de routage IPv6 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > IPv6 > Avancé > Configuration du préfixe**.

La page Configuration du préfixe s'affiche.

6. Dans le menu **interface**, sélectionnez l'interface.
7. Si vous modifiez un préfixe existant pour l'interface, cochez la case correspondant au préfixe.
8. Si vous ajoutez un nouveau préfixe, dans le champ **préfixe IPv6**, spécifiez le préfixe IPv6 de l'interface.
9. Si vous ajoutez un nouveau préfixe, dans le champ **longueur du préfixe**, spécifiez la longueur du préfixe IPv6 pour l'interface.
10. Dans le menu **EUI64**, sélectionnez **Activer** ou **désactiver** pour activer ou désactiver le préfixe monodiffusion 64 bits.
11. Dans le champ **durée de vie valide**, spécifiez la période de validité des annonces de préfixe de routeur pour l'interface.
Il s'agit de la période pendant laquelle le préfixe est valide aux fins de la détermination du lien. La plage est de 0 à 4294967295.
12. Dans le champ **durée de vie préférée**, spécifiez la période préférée pour les annonces de routeur de préfixe pour l'interface.
Il s'agit de la période pendant laquelle le préfixe est préféré aux fins de la détermination du lien. Une adresse autoconfigurée générée à partir du préfixe est une adresse préférée. La plage est de 0 à 4294967295.
13. Dans le menu **drapeau Onlink**, sélectionnez **Activer** ou **désactiver** pour activer ou désactiver l'utilisation du préfixe pour la configuration d'adresse autonome.
S'il est activé, le préfixe peut être utilisé pour la détermination sur liaison.
14. Dans le menu **drapeau autonome**, pour activer ou désactiver l'utilisation du préfixe pour la détermination sur liaison.
S'il est activé, le préfixe peut être utilisé pour la configuration d'adresse autonome.
15. Effectuez l'une des opérations suivantes :
 - Si vous ajoutez un nouveau préfixe, cliquez sur le bouton **Ajouter**.
Les paramètres sont enregistrés. Le préfixe est ajouté pour l'interface.
 - Si vous modifiez un préfixe existant, cliquez sur le bouton **appliquer**.
Les paramètres sont enregistrés.

Le champ Etat actuel affiche l'état de l'adresse IPV6. L'état est TENTE (provisoire) si le routage est désactivé ou si DAD (Duplicate Address Detection) échoue. L'état est actif si l'interface est active et que LE DAD réussit.
16. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimer un paramètre de préfixe d'une interface de routage IPv6

Vous pouvez supprimer un préfixe et les paramètres associés dont vous n'avez plus besoin pour une interface de routage IPv6.

Pour supprimer des paramètres de préfixe à partir d'une interface de routage IPv6 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > IPv6 > Avancé > Configuration du préfixe**.

La page Configuration du préfixe s'affiche.

6. Dans le menu **interface**, sélectionnez l'interface.
7. Cochez les cases correspondant au contenu.
8. Cliquez sur le bouton **Supprimer**.

Les paramètres sont enregistrés. Le préfixe est supprimé.

9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Afficher les statistiques IPv6 et ICMPv6 pour une interface de routage IPv6

Vous pouvez afficher les statistiques IPv6 et ICMPv6 pour une interface de routage IPv6.

Pour afficher les statistiques IPv6 et ICMPv6 pour une interface de routage IPv6 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > IPv6 > Avancé > statistiques**.

La page statistiques s'affiche.

6. Dans le menu **interface**, sélectionnez l'interface de routage IPv6.

7. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

Le tableau suivant décrit les champs en lecture seule de la section statistiques IPv6.

Table 114 : Informations statistiques de l'interface IPv6

Champ	Description
Nombre total de datagrammes reçus	Nombre total de datagrammes d'entrée reçus par l'interface, y compris ceux reçus par erreur
Datagrammes reçus livrés localement	Nombre total de datagrammes livrés avec succès aux protocoles utilisateur IPv6 (y compris ICMP). Ce compteur est incrémenté à l'interface à laquelle ces datagrammes ont été adressés, qui peut ne pas être l'interface d'entrée de certains datagrammes.
Datagrammes reçus rejetés en raison d'erreurs d'en-tête	Le nombre de datagrammes d'entrée rejetés en raison d'erreurs dans leurs en-têtes IPv6, y compris la discordance de numéro de version, d'autres erreurs de format, le nombre de sauts dépassé, les erreurs découvertes dans le traitement de leurs options IPv6, etc
Datagrammes reçus rejetés en raison de la MTU	Nombre de datagrammes d'entrée qui n'ont pas pu être transmis car leur taille dépassait la MTU de liaison de l'interface sortante
Datagrammes reçus rejetés en raison de l'absence de route	Nombre de datagrammes d'entrée rejetés car aucune route n'a pu être trouvée pour les transmettre à leur destination
Datagrammes reçus avec protocole inconnu	Nombre de datagrammes adressés localement reçus avec succès mais rejetés en raison d'un protocole inconnu ou non pris en charge. Ce compteur est incrémenté à l'interface à laquelle ces datagrammes ont été adressés, qui peut ne pas être l'interface d'entrée de certains datagrammes.
Datagrammes reçus rejetés en raison d'une adresse non valide	Nombre de datagrammes d'entrée ignorés car l'adresse IPv6 dans le champ de destination de leur en-tête IPv6 n'était pas une adresse valide à recevoir sur cette entité. Ce nombre inclut les adresses non valides (par exemple : :0) et les adresses non prises en charge (par exemple, les adresses avec des préfixes non alloués). Pour les entités qui ne sont pas des routeurs IPv6 et qui ne transmettent donc pas de datagrammes, ce compteur inclut les datagrammes rejetés car l'adresse de destination n'était pas une adresse locale.
Datagrammes reçus rejetés en raison de données tronquées	Nombre de datagrammes d'entrée rejetés car la trame de datagrammes ne transportait pas suffisamment de données
Datagrammes reçus ignorés autres	Nombre de datagrammes IPv6 d'entrée pour lesquels aucun problème n'a été rencontré pour empêcher leur traitement continu, mais qui ont été rejetés pour des raisons telles que le manque d'espace tampon. Ce compteur n'inclut pas les datagrammes jetés en attente de réassemblage.
Datagrammes reçus, réassemblage requis	Nombre de fragments IPv6 reçus qui devaient être réassemblés sur cette interface. Ce compteur est incrémenté à l'interface à laquelle ces fragments ont été adressés, qui peut ne pas être l'interface d'entrée de certains fragments.
Datagrammes remontés	Nombre de datagrammes IPv6 réassemblés avec succès. Ce compteur est incrémenté au niveau de l'interface à laquelle ces datagrammes ont été adressés, qui n'est peut-être pas nécessairement l'interface d'entrée de certains fragments.

Table 114 : Informations statistiques de l'interface IPv6 (A continué)

Champ	Description
Echec du réassemblage des datagrammes	Le nombre d'échecs détectés par l'algorithme de réassemblage IPv6 (pour une raison quelconque : expiration du délai, erreurs, etc.). Il ne s'agit pas nécessairement d'un comptage des fragments IPv6 rejetés puisque certains algorithmes (notamment l'algorithme de la RFC 815) peuvent perdre la trace du nombre de fragments en les combinant au fur et à mesure de leur réception. Ce compteur est incrémenté à l'interface à laquelle ces fragments ont été adressés, qui peut ne pas être l'interface d'entrée de certains fragments.
Datagrammes transmis	Nombre de datagrammes de sortie que cette entité a reçus et transmis à leurs destinations finales. Dans les entités qui n'agissent pas en tant que routeurs IPv6, ce compteur inclut uniquement les paquets qui ont été acheminés à la source via cette entité, et le traitement de la route source a réussi. Pour un datagramme transmis avec succès, le compteur de l'interface sortante est incrémenté.
Datagrammes transmis localement	Le nombre de datagrammes que cette entité a transmis avec succès à partir de cette interface de sortie.
Echec de la transmission des datagrammes	Le nombre de datagrammes que cette entité n'a pas réussi à transmettre
Datagrammes fragmentés	Nombre de datagrammes IPv6 fragmentés au niveau de cette interface de sortie
Echec du fragment des datagrammes	Nombre de datagrammes de sortie qui n'ont pas pu être fragmentés sur cette interface
Fragments de datagrammes créés	Nombre de fragments de datagramme de sortie générés à la suite de la fragmentation au niveau de cette interface de sortie
Datagrammes multidiffusion reçus	Nombre de paquets Hello reçus sur l'interface.
Datagrammes multicast transmis	Nombre de paquets OSPF transmis sur l'interface.

Le tableau suivant décrit les champs en lecture seule de la section statistiques ICMPv6.

Table 115 : Informations statistiques de l'interface ICMPv6

Champ	Description
Total des messages ICMPv6 reçus	Nombre total de messages ICMP reçus par l'interface, qui inclut tous ceux comptés par IPv6IfIcmpInErrors. Cette interface est l'interface à laquelle les messages ICMP ont été adressés, qui peut ne pas être l'interface d'entrée des messages.
Messages ICMPv6 avec erreurs reçus	Le nombre de messages ICMP reçus par l'interface mais identifiés comme présentant des erreurs spécifiques à ICMP (sommes de contrôle ICMP erronées, longueur incorrecte, etc.)
ICMPv6 destination inaccessible messages reçus	Nombre de messages ICMP destination inaccessible reçus par l'interface

Table 115 : Informations statistiques de l'interface ICMPv6 (A continué)

Champ	Description
ICMPv6 messages interdits administrativement reçus	Nombre de messages de destination ICMP inaccessibles/de communication administrativement interdits reçus par l'interface
ICMPv6 - délai dépassé messages reçus	Le nombre de messages de dépassement de temps ICMP reçus par l'interface
Messages de problème de paramètre ICMPv6 reçus	Nombre de messages de problème de paramètre ICMP reçus par l'interface
ICMPv6 paquets trop volumineux messages reçus	Nombre de messages ICMP paquet trop volumineux reçus par l'interface
Messages de demande d'écho ICMPv6 reçus	Nombre de messages ICMP Echo (requête) reçus par l'interface
Messages de réponse écho ICMPv6 reçus	Nombre de messages de réponse écho ICMP reçus par l'interface
Messages de sollicitation du routeur ICMPv6 reçus	Nombre de messages de sollicitation du routeur ICMP reçus par l'interface
Messages publicitaires du routeur ICMPv6 reçus	Nombre de messages d'annonce de routeur ICMP reçus par l'interface
Messages ICMPv6 de sollicitation de voisins reçus	Nombre de messages ICMP Neighbor Request reçus par l'interface
Messages d'annonce de voisinage ICMPv6 reçus	Nombre de messages d'annonce de voisinage ICMP reçus par l'interface
Messages de redirection ICMPv6 reçus	Nombre de messages de redirection ICMPv6 reçus par l'interface
Messages de requête d'appartenance au groupe ICMPv6 reçus	Nombre de messages ICMPv6 Group Membership Query reçus par l'interface
Messages de réponse d'appartenance au groupe ICMPv6 reçus	Nombre de messages de réponse d'appartenance à un groupe ICMPv6 reçus par l'interface
Messages ICMPv6 de réduction de l'appartenance au groupe reçus	Le nombre de messages ICMPv6 Group Membership Reduction reçus par l'interface
Total des messages ICMPv6 transmis	Nombre total de messages ICMP que cette interface a tenté d'envoyer. Ce compteur inclut tous ceux comptés par icmpOutErrors.
Messages ICMPv6 non transmis en raison d'une erreur	Nombre de messages ICMP que cette interface n'a pas envoyés en raison de problèmes découverts dans ICMP, tels qu'un manque de tampons. Cette valeur n'inclut pas les erreurs découvertes en dehors de la couche ICMP, telles que l'incapacité d'IPv6 à acheminer le datagramme résultant. Dans certaines implémentations, il peut n'y avoir aucun type d'erreur qui contribue à la valeur de ce compteur.
ICMPv6 destination inaccessible messages transmis	Nombre de messages ICMP destination inaccessible envoyés par l'interface

Table 115 : Informations statistiques de l'interface ICMPv6 (A continué)

Champ	Description
ICMPv6 messages interdits administrativement transmis	Nombre de messages de destination ICMP inaccessibles/communication administrativement interdite envoyés
ICMPv6 - délai dépassé messages transmis	Le nombre de messages ICMP dépassés envoyés par l'interface
Messages de problème de paramètre ICMPv6 transmis	Nombre de messages de problème de paramètre ICMP envoyés par l'interface
ICMPv6 paquets trop volumineux messages transmis	Nombre de messages ICMP Packet Too Big envoyés par l'interface
Messages de demande d'écho ICMPv6 transmis	Nombre de messages ICMP Echo (requête) envoyés par l'interface
Messages de réponse écho ICMPv6 transmis	Nombre de messages de réponse écho ICMP envoyés par l'interface
Le routeur ICMPv6 sollicite les messages transmis	Nombre de messages de sollicitation de voisins ICMP envoyés par l'interface
Messages publicitaires du routeur ICMPv6 transmis	Nombre de messages d'annonce de routeur ICMP envoyés par l'interface
ICMPv6 messages de sollicitation de voisins transmis	Nombre de messages de sollicitation de voisins ICMP envoyés par l'interface
Messages d'annonce de voisinage ICMPv6 transmis	Nombre de messages d'annonce de voisinage ICMP envoyés par l'interface
ICMPv6 Redirect messages transmis	Nombre de messages de redirection envoyés
Messages de requête d'appartenance au groupe ICMPv6 transmis	Nombre de messages de requête d'appartenance à un groupe ICMPv6 envoyés
Messages de réponse d'appartenance au groupe ICMPv6 transmis	Nombre de messages de réponse d'appartenance à un groupe ICMPv6 envoyés
Messages ICMPv6 de réduction de l'appartenance au groupe transmis	Nombre de messages ICMPv6 de réduction de l'appartenance à un groupe envoyés
ICMPv6 adresse dupliquée détectée	Nombre d'adresses dupliquées détectées par l'interface

Affichez la table de voisinage IPv6 ou effacez les entrées de voisinage IPv6

Vous pouvez afficher les périphériques voisins IPv6 détectés par le commutateur ou effacer les entrées de voisins IPv6 de la table de voisins.

Pour afficher la table de voisins IPv6 ou effacer les entrées de voisins IPv6 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > IPv6 > Avancé > table de voisinage** .

La page table de voisinage OSPFv3 s'affiche.

6. Dans le menu **Rechercher par**, sélectionnez l'une des méthodes suivantes pour rechercher des voisins IPv6 :

- Adresse IPv6 : Entrez l'adresse IPv6 hexadécimale de 128 octets dans des groupes de quatre chiffres séparés par deux-points, par exemple, 2001 :231F :: :1. Cliquez

ensuite sur le bouton **aller**. Si l'adresse existe, cette entrée s'affiche. Une correspondance exacte est requise.

- Interface Entrez l'ID d'interface au format unité/port, par exemple, 0/4. Cliquez ensuite sur le bouton **aller**. Si l'adresse existe, cette entrée s'affiche.
7. Pour effacer les voisins IPv6 qui s'affichent, cliquez sur le bouton **Effacer**.
 8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.
 9. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

Le tableau suivant décrit les champs en lecture seule de la page.

Table 116 : Table de voisinage avancée IPv6

Champ	Description
Interface	Interface pour laquelle les paramètres sont affichés
Adresse IPv6	Adresse IPv6 du voisin ou de l'interface
Adresse MAC	Adresse MAC associée à une interface
IsRtr	Indique si le voisin est un routeur. Si le voisin est un routeur, le champ affiche vrai. Si le voisin n'est pas un routeur, le champ affiche faux.
Etat voisin	État de l'entrée du cache voisin. Voici les états des entrées dynamiques dans le cache de découverte de voisins IPv6 : • Incmp : La résolution d'adresse est en cours d'exécution sur l'entrée. Un message de sollicitation de voisin a été envoyé à l'adresse de multidiffusion de noeud sollicité de la cible, mais le message d'annonce de voisin correspondant n'a pas encore été reçu. • Portée : Une confirmation positive a été reçue dans les dernières millisecondes "ReachableTime" que le chemin vers le voisin fonctionnait correctement. Dans l'état REACH, le périphérique n'effectue aucune action particulière lorsque des paquets sont envoyés. • Périmé : Plus de millisecondes que le « ReachableTime » se sont écoulées depuis la dernière confirmation positive que le chemin avant fonctionnait correctement. Lorsqu'il est PÉRIMÉ, le périphérique n'effectue aucune action jusqu'à ce qu'un paquet soit envoyé. • Délai : Plus de « ReachableTime » millisecondes se sont écoulées depuis la dernière confirmation positive que le chemin avant fonctionnait correctement. Un paquet a été envoyé au cours des dernières secondes DELAY_FIRST_PROBE_TIME. Si aucune confirmation d'accessibilité n'est reçue dans les secondes DELAY_FIRST_PROBE_TIME suivant l'entrée dans l'état DELAY, envoyez un message de sollicitation de voisin et changez l'état en SONDÉ. • Sonde : Une confirmation d'accessibilité est activement recherchée en renvoyant des messages de sollicitation de voisins toutes les millisecondes « RetransTimer » jusqu'à ce qu'une confirmation d'accessibilité soit reçue.
Dernière mise à jour	Temps écoulé depuis que l'adresse a été confirmée pour être joignable

Configurer les routes statiques IPv6

Vous pouvez ajouter ou modifier une route IPv6 statique.

Pour ajouter ou modifier une route IPv6 statique :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > IPv6 > Avancé > Configuration statique de l'itinéraire**.

La page Configuration d'itinéraire statique s'affiche.

6. Si vous modifiez un itinéraire existant, cochez la case de l'itinéraire.

Le seul champ que vous pouvez modifier est la préférence pour l'itinéraire.

7. Si vous ajoutez une nouvelle route, dans le champ **préfixe IPv6**, spécifiez le préfixe IPv6 de la route.

8. Si vous ajoutez une nouvelle route, dans le champ **longueur du préfixe**, spécifiez la longueur du préfixe IPv6 pour la route.

9. Si vous ajoutez une nouvelle route, dans le menu **type d'adresse IPv6 de saut suivant**, sélectionnez l'une des options suivantes :

- **Global** : Créez une route IPv6 globale en spécifiant l'interface de la route.
 - **Lien-local** : Créez une adresse IPv6 lien-local en spécifiant l'interface et l'adresse de saut suivant pour la route.
 - **Rejet statique** : Créez une route de rejet statique pour un préfixe de destination. Vous ne pouvez pas spécifier une interface ou une adresse de saut suivant pour la route.
10. Si vous ajoutez une nouvelle route et que vous avez sélectionné **Global** ou **Link-local** dans le menu **type d'adresse IPv6 du saut suivant**, spécifiez l'adresse IPv6 du saut suivant dans le champ **adresse IPv6 du saut suivant**.
 11. Si vous ajoutez une nouvelle route et que vous avez sélectionné **lien-local** dans le menu **type d'adresse IPv6 de saut suivant**, spécifiez l'interface de la route.
 12. Dans le champ **préférence**, spécifiez la préférence de l'itinéraire.
La plage est de 1 à 255. Vous pouvez ajouter la préférence pour un nouvel itinéraire ou modifier la préférence pour un itinéraire existant.
 13. Effectuez l'une des opérations suivantes :
 - Si vous ajoutez une nouvelle route, cliquez sur le bouton **Ajouter**.
Les paramètres sont enregistrés. La route est ajoutée.
 - Si vous modifiez un itinéraire existant, cliquez sur le bouton **appliquer**.
Les paramètres sont enregistrés.
 14. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimer une route statique IPv6

Vous pouvez supprimer une route statique IPv6 dont vous n'avez plus besoin.

Pour supprimer une route statique IPv6 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **routing > IPv6 > Avancé > Configuration statique de l'itinéraire** .
La page Configuration d'itinéraire statique s'affiche.
6. Cochez les cases correspondant au contenu.
7. Cliquez sur le bouton **Supprimer**.
Les paramètres sont enregistrés. La route est supprimée.
8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez la préférence de route IPv6 pour le commutateur

Vous pouvez configurer la préférence par défaut pour le commutateur, qui est une valeur comprise entre 1 et 255 et indépendante des mesures de route. La plupart des protocoles de routage utilisent une métrique de route pour déterminer le chemin le plus court connu du protocole, indépendamment de tout autre protocole. Le meilleur itinéraire vers une destination est automatiquement sélectionné en déterminant l'itinéraire avec la valeur de préférence la plus basse. S'il existe plusieurs routes vers une destination, la valeur de préférence est utilisée pour déterminer la route préférée. Si une égalité se produit, l'itinéraire avec la meilleure métrique d'itinéraire est sélectionné.

Configurez la préférence de route IPv6 pour le commutateur :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > IPv6 > Avancé > préférence d'itinéraire**.

La page Préférences d'itinéraire s'affiche.

6. Dans le champ **statique**, spécifiez la valeur de préférence de route statique pour le commutateur

La plage est de 1 à 255. La valeur par défaut est 1.

7. Dans le champ **OSPFv3 intra**, spécifiez la préférence de route OSPFv3 intra sur le commutateur.

La valeur par défaut est 110. La plage est de 1 à 255.

8. Dans le champ **Inter OSPFv3**, spécifiez la préférence inter route OSPFv3 sur le commutateur.

La valeur par défaut est 110. La plage est de 1 à 255.

9. Dans le champ **externe OSPFv3**, spécifiez la préférence de route externe OSPFv3 sur le commutateur.

La valeur par défaut est 110. La plage est de 1 à 255.

10. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

Le champ local affiche la préférence locale.

11. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

VLAN de routage

Vous pouvez configurer certaines interfaces pour prendre en charge les VLAN et d'autres interfaces pour prendre en charge le routage. Vous pouvez également configurer un VLAN pour qu'il fonctionne comme si informatique était une interface de routage.

Lorsqu'une interface est activée pour le pontage (paramètre par défaut) plutôt que pour le routage, tout le traitement de pont normal est effectué pour un paquet entrant, qui est ensuite associé à un VLAN. Son adresse MAC de destination (MAC DA) et son ID VLAN sont utilisés pour effectuer des recherches dans la table d'adresses MAC. Si le routage est activé pour le VLAN et que le MAC DA d'un paquet de monodiffusion entrant est celui de l'interface pont-routeur interne, le paquet est routé. Un paquet de multidiffusion entrant est transmis à tous les ports du VLAN, ainsi qu'à l'interface pont-routeur interne, si le informatique a été reçu sur un VLAN routé.

Étant donné qu'une interface peut appartenir à plusieurs VLAN, le routage VLAN peut être activé pour tous les VLAN de l'interface ou pour un sous-ensemble. Le routage VLAN peut être utilisé pour permettre à plusieurs ports physiques de résider sur le même sous-réseau. informatique peut également être utilisé lorsqu'un VLAN s'étend sur plusieurs réseaux physiques, ou lorsqu'une segmentation ou une sécurité supplémentaire est requise.

Une interface peut être une interface VLAN ou une interface de routage, mais pas les deux. Cependant, une interface VLAN peut faire partie d'un VLAN qui fonctionne comme une interface de routage.

Créez un VLAN de routage à l'aide de l'assistant de routage statique VLAN

L'assistant de routage statique VLAN vous permet de créer un VLAN et d'ajouter des interfaces au VLAN. L'assistant de routage statique VLAN vous permet également d'ajouter des interfaces sélectionnées en tant que groupe d'agrégation de liens (lag). Avec l'assistant, vous pouvez effectuer les opérations suivantes :

- Créez un VLAN et générez un nom unique pour VLAN.
- Ajoutez les interfaces sélectionnées au VLAN nouvellement créé ou supprimez les interfaces sélectionnées du VLAN par défaut.

- Ajoutez les interfaces sélectionnées à un lag et ajoutez le lag à un VLAN nouvellement créé.
- Activez le balisage sur les interfaces sélectionnées si l'interface est membre d'un autre VLAN. Vous pouvez également désactiver le balisage si l'interface sélectionnée n'est pas membre d'un autre VLAN.
- Exclure des ports du VLAN.
- Activez le routage sur VLAN et spécifiez une adresse IP et un masque de sous-réseau pour le routage.

Pour créer un VLAN de routage à l'aide de l'assistant de routage statique VLAN :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > VLAN > Assistant routage statique VLAN** .

La page Assistant routage statique VLAN s'affiche.

Les ports du commutateur (unité 1) sont affichés. Si une pile est configurée, les ports de chaque commutateur empilé (unité 1, unité 2, etc.) sont affichés. En outre, tous les LAG sont affichés, qu'une pile soit configurée ou non.

6. Dans le champ **VLAN ID**, spécifiez l'identifiant VLAN (VID) qui doit être associé au VLAN.

La plage est de 1 à 4093.

7. Dans le champ **adresse IP**, spécifiez l'adresse IPv4 de l'interface de routage VLAN.
8. Dans le champ **masque réseau**, spécifiez le masque de sous-réseau de l'interface de routage VLAN.
9. Dans la table ports (ou, si une pile est configurée, dans l'une des tables ports), cliquez une, deux ou trois fois sur un port pour configurer l'un des modes suivants :

- **T (marqué) membre** : Le port est ajouté en tant que membre balisé du VLAN.
- **Membre U (non étiqueté)** : Le port est ajouté en tant que membre non balisé du VLAN.
- **Membre exclu** : Par défaut, la sélection est vide, ce qui signifie que le port est exclu du VLAN. Un port exclu peut toujours être ajouté dynamiquement au VLAN via GVRP.

Si une pile est configurée, vous pouvez sélectionner des ports dans plusieurs tables.

10. Dans le tableau lag, cliquez une fois, deux fois ou trois fois sur un lag pour configurer l'un des modes suivants :

- **T (marqué) membre** : Le lag est ajouté en tant que membre balisé du VLAN.
- **Membre U (non étiqueté)** : Le lag est ajouté en tant que membre non balisé du VLAN.
- **Membre exclu** : Par défaut, la sélection est vide, ce qui signifie que le lag est exclu du VLAN. Un lag exclu peut toujours être ajouté dynamiquement au VLAN via GVRP.

11. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

12. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurer le routage pour un VLAN existant

Pour un VLAN existant, vous pouvez ajouter ou modifier une adresse IPv4 et un masque de sous-réseau et configurer le routage pour le VLAN.

Pour ajouter ou modifier le routage d'un VLAN existant :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > VLAN > Configuration du routage VLAN**.

La page routage VLAN s'affiche.

6. Si vous modifiez une VLAN de routage existante, cochez la case VLAN.

7. Si vous ajoutez une nouvelle VLAN de routage, dans le menu **VLAN ID**, sélectionnez VLAN ID.

Ce menu affiche les ID de tous les VLAN configurés sur ce commutateur.

8. Dans le champ **adresse IP**, spécifiez l'adresse IP de l'VLAN de routage.

9. Dans le champ **masque de sous-réseau**, spécifiez le masque de sous-réseau de l'VLAN de routage.

10. Effectuez l'une des opérations suivantes :

- Si vous ajoutez une nouvelle VLAN de routage, cliquez sur le bouton **Ajouter**. Les paramètres sont enregistrés. L'VLAN de routage est ajouté.
- Si vous modifiez une VLAN de routage existante, cliquez sur le bouton **appliquer**.

Les paramètres sont enregistrés.

11. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 117 : Informations de configuration du routage VLAN

Champ	Description
Port	Interface pour le VLAN de routage.
Adresse MAC	Adresse MAC de l'interface pour le VLAN de routage.

Supprimez la fonction de routage d'un VLAN

Vous pouvez supprimer la fonction de routage d'un VLAN. Autrement dit, vous pouvez supprimer l'adresse IP de routage et le masque de sous-réseau du VLAN. Le VLAN lui-même n'est pas supprimé.

Pour supprimer la fonction de routage d'un VLAN :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > VLAN > Configuration du routage VLAN**.

La page routage VLAN s'affiche.

6. Cochez les cases correspondant au contenu.

7. Cliquez sur le bouton **Supprimer**.

Les paramètres sont enregistrés. La fonction de routage est supprimée du VLAN mais le VLAN lui-même n'est pas supprimé.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Protocole de résolution d'adresse

Le protocole ARP (Address Resolution Protocol) associe une adresse MAC de couche 2 à une adresse IPv4 de couche 3. Le commutateur prend en charge une configuration ARP dynamique et manuelle. Avec la configuration ARP manuelle, vous pouvez ajouter statiquement des entrées dans la table ARP.

Le protocole ARP est une partie obligatoire du protocole Internet (IP) et est utilisé pour traduire une adresse IP en une adresse de support (MAC), définie par un LAN tel qu'un LAN Ethernet. Une unité qui envoie des paquets IP doit apprendre l'adresse MAC de la destination IP ou du routeur du tronçon suivant, si la destination ne se trouve pas sur le même sous-réseau. Ceci est réalisé par diffusion d'un paquet de requête ARP, auquel le destinataire prévu répond en diffusant à l'unité une réponse ARP contenant son adresse MAC. Une fois apprise, l'adresse MAC est utilisée dans le champ d'adresse de destination de l'en-tête de couche 2 préfixé au paquet IP.

Le cache ARP est une table gérée localement sur chaque périphérique d'un réseau. Les entrées de cache ARP sont apprises en examinant les informations source dans les champs de charge utile du paquet ARP, que informatique soit une requête ou une réponse ARP. Ainsi, lorsqu'une requête ARP est diffusée sur tous les périphériques d'un réseau local ou VLAN, chaque destinataire peut stocker l'adresse IP et MAC de l'expéditeur dans son cache ARP respectif. La réponse ARP (qui est un message unicast) est normalement détectée uniquement par le demandeur, qui stocke les informations de l'expéditeur dans son cache ARP. Les informations les plus récentes remplacent toujours le contenu existant dans le cache ARP.

Le nombre d'entrées ARP prises en charge dépend du périphérique.

Un périphérique peut être déplacé dans un réseau, ce qui signifie que l'adresse IP du périphérique qui était associée à une adresse MAC est maintenant associée à une autre adresse MAC. Un périphérique peut également disparaître complètement du réseau

(par exemple, informatique a été reconfiguré, déconnecté ou éteint). Ces situations entraînent des informations obsolètes dans le cache ARP. Par conséquent, les entrées sont mises à jour ou périodiquement actualisées pour déterminer si une adresse existe toujours. Si une entrée a été identifiée comme expéditeur d'un paquet ARP, elle peut être supprimée du cache ARP. Vous pouvez configurer un intervalle d'expiration qui détermine la durée pendant laquelle une entrée non mise à jour reste dans le cache ARP.

Affiche les entrées ARP dans le cache ARP

Vous pouvez afficher les entrées ARP dans le cache ARP. Le cache ARP est un tableau qui répertorie les connexions distantes récemment détectées par le commutateur

Pour afficher les entrées ARP dans le cache ARP :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > ARP > basique > cache ARP**.

La page cache ARP s'affiche.

La page journaux affiche les informations suivantes :

- **IP Address** (Adresse IP). Affiche l'adresse IP associée à l'adresse MAC du système. Cette adresse doit être l'adresse IP d'un périphérique sur un sous-réseau connecté à l'une des interfaces de routage existantes du commutateur.
- **Port**. Affiche l'unité/logement/port associé à la connexion.
- **MAC Address** (Adresse IP). Affiche l'adresse MAC monodiffusion du périphérique. L'adresse est composée de six nombres hexadécimaux à 2 chiffres séparés par deux-points, par exemple 00 :06 :29 :32 :81 :40.

Le cache ARP est volumineux. Le menu de navigation de pagination fonctionne comme suit :

- Lignes par page : Sélectionnez le nombre d'entrées de table affichées par page. Les valeurs possibles sont 20, 50, 100, 200 et tous. Si vous sélectionnez tout, le navigateur peut être lent à afficher les informations.
- <. Affiche la page précédente des entrées de données du tableau.
- >. Affiche la page suivante des entrées de données du tableau.

6. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

Ajoutez ou modifiez une entrée statique dans la table ARP

Vous pouvez ajouter une nouvelle entrée statique à la table ARP ou modifier une entrée existante que vous avez ajoutée manuellement.

Pour ajouter une nouvelle entrée statique ou modifier une entrée existante dans la table ARP :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > ARP > Avancé > créer ARP**.

La page créer ARP s'affiche.

6. Si vous modifiez une entrée ARP existante, cochez la case correspondante.

7. Dans le champ **adresse IP**, spécifiez l'adresse IP à ajouter.

L'adresse doit être l'adresse IP d'un périphérique sur un sous-réseau connecté à l'une des interfaces de routage existantes du commutateur.

8. Dans le champ **adresse MAC**, spécifiez l'adresse MAC monodiffusion du périphérique.

Entrez l'adresse sous la forme de six nombres hexadécimaux à 2 chiffres séparés par deux points, par exemple 00 :06 :29 :32 :81 :40.

9. Effectuez l'une des opérations suivantes :

- Si vous ajoutez une nouvelle entrée ARP, cliquez sur le bouton **Ajouter**.
Les paramètres sont enregistrés. L'entrée ARP est ajoutée.
- Si vous modifiez une entrée ARP existante, cliquez sur le bouton **appliquer**.
Les paramètres sont enregistrés.

10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

La table ARP peut être grande. Le menu de navigation de pagination fonctionne comme suit :

- Lignes par page : Sélectionnez le nombre d'entrées de table affichées par page. Les valeurs possibles sont 20, 50, 100, 200 et tous. Si vous sélectionnez tout, le navigateur peut être lent à afficher les informations.
- <. Affiche la page précédente des entrées de données du tableau.
- >. Affiche la page suivante des entrées de données du tableau.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 118 : Informations sur le cache ARP

Champ	Description
Adresse IP	Adresse IP du périphérique connecté.
Port	Interface associée (au format unité/port) pour la connexion du périphérique.
Adresse MAC	Adresse MAC de monodiffusion du périphérique.
Type	Type d'entrée ARP. Les valeurs possibles sont les suivantes : • Local Entrée ARP associée à l'une des adresses MAC de l'interface de routage du commutateur. • Passerelle : Entrée ARP dynamique dont l'adresse IP est celle d'un routeur. • Statique Une entrée ARP que vous avez ajoutée. • Dynamique Entrée ARP apprise par le commutateur.
Age :	Temps (en secondes) écoulé depuis la dernière actualisation de l'entrée dans la table ARP.

Supprimer une entrée ARP statique

Vous pouvez supprimer une entrée ARP statique dont vous n'avez plus besoin.

Pour supprimer une entrée ARP statique :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > ARP > Avancé > créer ARP**.

La page créer ARP s'affiche.

6. Cochez les cases correspondant au contenu.

7. Cliquez sur le bouton **Supprimer**.

Les paramètres sont enregistrés. L'entrée est supprimée.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez les paramètres de la table ARP ou supprimez des entrées de la table

Vous pouvez modifier les paramètres de configuration de la table ARP. Vous pouvez également supprimer des entrées de la table, par exemple, toutes les entrées dynamiques.

Pour configurer les paramètres de la table ARP ou supprimer des entrées de la table :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.
4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **routage > ARP > Avancé > Configuration ARP globale** .
La page Configuration ARP globale s'affiche.
6. Dans le champ **Age Time**, spécifiez la période en secondes pendant laquelle une entrée ARP dynamique reste dans la table ARP avant expiration.
La plage est de 15 à 21600 secondes. La valeur par défaut est de 1200 secondes.
7. Dans le champ **temps de réponse**, spécifiez la période en secondes pendant laquelle le commutateur attend une réponse ARP à une requête ARP envoyée par informatique.
La plage est de 1 à 10 secondes. La valeur par défaut est 1 seconde.
8. Dans le champ **tentatives**, spécifiez le nombre maximal de tentatives d'une demande ARP après que le commutateur n'a pas reçu de réponse ARP.
Ce numéro inclut la demande ARP initiale. La plage est de 0 à 10. Le numéro par défaut est 4.
9. Dans le champ **taille du cache**, spécifiez le nombre maximal d'entrées autorisées dans la table ARP.
Ce nombre inclut toutes les entrées ARP statiques et dynamiques. La plage est comprise entre 384 et 760. Le numéro par défaut est 760.
10. Sélectionnez le bouton radio **Activer** ou **désactiver** le renouvellement dynamique pour activer ou désactiver les entrées ARP dynamiques afin de tenter d'être renouvelées automatiquement après expiration.
La valeur par défaut est Activer.
11. Pour supprimer certaines entrées de la table ARP, sélectionnez l'une des options suivantes dans le menu **Supprimer de la table** :

- **Toutes les entrées dynamiques** : Toutes les entrées dynamiques seront supprimées.
- **Toutes les entrées dynamiques et de passerelle** : Toutes les entrées dynamiques et de passerelle seront supprimées.
- **Entrée dynamique/passerelle spécifique** : Vous devez spécifier l'adresse IP de l'entrée dynamique spécifique ou de l'entrée de passerelle spécifique dans le champ **Supprimer l'adresse IP**.
- **Saisie statique spécifique** : Vous devez spécifier l'adresse IP de l'entrée statique spécifique dans le champ **Supprimer l'adresse IP**.

12. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

13. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 119 : Configuration de la table ARP

Champ	Description
Nombre total d'entrées	Nombre total d'entrées dans la table ARP
Nombre total d'entrées de pointe	La valeur la plus élevée atteinte dans le champ nombre total d'entrées. Ce compteur est redémarré lorsque vous modifiez la taille du cache de la table ARP.
Entrées statiques actives	Nombre total d'entrées statiques actives dans la table ARP
Entrées statiques configurées	Nombre total d'entrées statiques configurées dans la table ARP
Nombre maximal d'entrées statiques	Nombre maximal d'entrées statiques pouvant être définies

Protocole d'informations de routage

Le protocole RIP (Routing information Protocol) est un protocole que les commutateurs et les routeurs peuvent utiliser pour échanger des informations de topologie réseau. Le protocole RIP est caractérisé comme un protocole de passerelle intérieure et est généralement utilisé dans les réseaux de petite et moyenne taille. Un périphérique qui exécute le protocole RIP envoie le contenu de sa table de routage à chacun de ses périphériques adjacents. Lorsqu'une route est supprimée de la table de routage,

informatique est marqué comme inutilisable par les autres périphériques et, après un certain temps, supprimé de leur routage.

Il existe deux versions de RIP :

- **RIPv1 (défini dans la RFC 1058) :**
 - Les routes sont spécifiées par le réseau de destination IP et le nombre de sauts
 - La table de routage est diffusée vers tous les périphériques du réseau connecté
- **RIPv2 (défini dans la RFC 1723) :**
 - La spécification de route inclut également le masque de sous-réseau et la passerelle
 - La table de routage est envoyée à une adresse de multidiffusion, ce qui réduit le trafic réseau
 - L'authentification est utilisée pour la sécurité

Vous pouvez configurer une interface pour effectuer les opérations suivantes :

- Recevez des paquets dans l'un ou l'autre des formats ou dans les deux
- Envoyez des paquets formatés pour RIPv1 ou RIPv2, ou envoyez des paquets RIPv2 à l'adresse de diffusion RIPv1
- Empêcher la réception de paquets RIP
- Empêcher l'envoi de paquets RIP

Activez ou désactivez le protocole RIP sur le commutateur

Par défaut, le protocole RIP est activé sur le commutateur.

Pour activer ou désactiver le protocole RIP sur le commutateur :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > RIP > basique > Configuration RIP**.

L'écran RIP Configuration (Configuration IP) s'affiche.

6. Sélectionnez le bouton radio **Activer** ou **désactiver** le mode d'administration RIP pour activer ou désactiver le protocole RIP sur le commutateur.

La valeur par défaut est Activer.

7. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez les paramètres RIP globaux du commutateur

Vous pouvez configurer les paramètres RIP globaux du commutateur, par opposition aux paramètres RIP des interfaces individuelles.

Pour configurer les paramètres RIP globaux du commutateur :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **routage > RIP > Avancé > Configuration RIP** .
L'écran RIP Configuration (Configuration IP) s'affiche.
6. Sélectionnez le bouton radio **Activer** ou **désactiver** le mode d'administration RIP pour activer ou désactiver le protocole RIP sur le commutateur.
La valeur par défaut est Activer.
7. Sélectionnez l'un des boutons radio mode Horizon partagé suivants :
 - Aucun : Aucun traitement spécial n'est activé.
 - Tranquillité d'esprit Une route n'est pas incluse dans les mises à jour envoyées au périphérique à partir duquel l'information a été apprise. La valeur par défaut est simple.
 - Poison Reverse Une route est incluse dans les mises à jour envoyées au périphérique à partir duquel l'information a été apprise, mais la métrique est définie sur infini.

Split horizon est une technique pour prévenir les problèmes qui pourraient être causés par l'inclusion de routes dans les mises à jour envoyées à un périphérique à partir duquel la route a été initialement apprise.

8. Sélectionnez le bouton radio **Activer** ou **désactiver** le mode de résumé automatique pour activer ou désactiver le résumé de groupes de routes adjacentes en entrées uniques.
Si vous sélectionnez le bouton radio **Activer**, les routes adjacentes sont résumées en entrées uniques afin de réduire le nombre total d'entrées. La valeur par défaut est désactiver.

9. Sélectionnez le bouton radio Host routes Accept mode **Enable** ou **Disable** pour activer ou désactiver l'acceptation des routes hôte par le commutateur.
Si vous sélectionnez le bouton radio **Activer**, le commutateur accepte les routes hôte. La valeur par défaut est Activer.
10. Sélectionnez le bouton radio Default information Origin **Activer** ou **désactiver** pour activer ou désactiver les annonces d'itinéraire par défaut.
La valeur par défaut est désactiver.
11. Dans le champ **métrique par défaut**, spécifiez une valeur métrique pour les routes redistribuées.
La plage est de 1 à 15. Le numéro par défaut est 0.
12. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
13. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 120 : Informations de configuration RIP

Champ	Description
Modifications globales de l'itinéraire	Nombre de modifications de route apportées à la base de données de routes IP par le protocole RIP. Cela n'inclut pas l'actualisation d'une route après expiration de informatique.
Requêtes globales	Nombre de réponses envoyées aux requêtes RIP à partir d'autres périphériques.

Configurer les paramètres de l'interface RIP

Vous pouvez configurer les paramètres RIP qui s'appliquent à des interfaces individuelles.

Pour configurer les paramètres de l'interface RIP :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > RIP > Avancé > Configuration de l'interface**.

La page Configuration de l'interface s'affiche.

6. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :

- **1 ou ID d'unité pour un commutateur empilé :**

- 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
- **ID d'unité pour un commutateur empilé :** Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.

- VLAN Seuls les VLAN sont affichés.

- **Tous:** Les interfaces physiques et les VLAN sont affichés, ou pour une pile de commutateurs, les interfaces physiques et les VLAN de tous les commutateurs sont affichés.

7. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :

- Pour afficher ou effacer les statistiques d'une seule interface, cochez la case associée à l'interface ou saisissez le numéro de l'interface dans le champ **aller à l'interface** et cliquez sur le bouton **aller**.
- Pour configurer plusieurs interfaces avec les mêmes paramètres, cochez la case associée à chaque interface.
- Pour configurer toutes les interfaces avec les mêmes paramètres, cochez la case dans la ligne d'en-tête.

8. Dans le menu **Send version**, sélectionnez la version des paquets de contrôle RIP que l'interface envoie :

- **Néant.** Aucun paquet de contrôle RIP n'est envoyé.
 - **RIP-1** : Envoie des paquets formatés RIP version 1 par diffusion.
 - **RIP-1c** : Envoyer des paquets en mode de compatibilité RIP version 1 et envoyer des paquets formatés RIP version 2 par diffusion.
 - **RIP-2** : Envoyer des paquets RIP version 2 en utilisant la multidiffusion. La valeur par défaut est RIP-2.
9. Dans le menu **Receive version**, sélectionnez la version des paquets de contrôle RIP que l'interface accepte :
- **RIP-1** : Accepter uniquement les paquets formatés RIP version 1.
 - **RIP-2** : Accepter uniquement les paquets formatés RIP version 2.
 - **Les deux** : Acceptez les paquets au format RIP version 1 ou RIP version 2. La valeur par défaut est les deux.
 - **Aucun** : Aucun paquet de contrôle RIP n'est accepté.
10. Dans le menu **mode RIP**, sélectionnez **Activer** ou **désactiver** pour activer ou désactiver le mode RIP de l'interface.
- Avant d'activer le protocole RIP version 1 ou version 1c sur une interface, vous devez d'abord activer le mode de diffusion dirigé vers le réseau (c'est-à-dire le mode RIP) sur l'interface. La valeur par défaut est désactiver.
11. Dans le menu **type de fichier**, sélectionnez le type de fichier :
- **Aucun** : Aucun protocole d'authentification n'est configuré. Il s'agit de l'option par défaut.
 - **Tranquillité d'esprit** Vous êtes invité à saisir une clé d'authentification. Cette clé est incluse (au format non chiffré) dans l'en-tête RIP de tous les paquets envoyés sur le réseau. Tous les périphériques du réseau doivent être configurés avec la même clé.
 - **Chiffrement** Vous êtes invité à saisir une clé d'authentification et un ID d'authentification. Le chiffrement utilise l'algorithme MD5 message-Digest. Tous les périphériques du réseau doivent être configurés avec la même clé et le même ID.
12. Si vous sélectionnez **simple** ou **crypter** dans le menu type d'authentification, dans le champ **clé d'authentification**, saisissez la clé d'authentification RIP de l'interface. La clé peut avoir jusqu'à 16 octets de long.
13. Si vous sélectionnez **crypter** dans le menu Authentication type, dans le champ **Authentication Key ID**, entrez l'ID de la clé d'authentification RIP pour l'interface. L'ID de clé peut être compris entre 0 et 255.
14. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

15. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

16. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 121 : Informations de configuration de l'interface RIP

Champ	Description
Paquets incorrects reçus	Nombre de paquets de réponse RIP reçus par le processus RIP qui ont ensuite été rejetés pour une raison quelconque
Mauvais itinéraires reçus	Nombre de routes dans des paquets RIP valides qui ont été ignorées pour une raison quelconque (par exemple, famille d'adresses inconnue ou métrique non valide)
Mises à jour LS envoyées	Nombre de mises à jour RIP déclenchées envoyées sur l'interface. Cela n'inclut pas explicitement les mises à jour complètes envoyées contenant de nouvelles informations.
Adresse IP	Adresse IP de l'interface réseau.
Etat du lien	Indique si l'interface du routeur RIP est active ou inactive

Configurez les paramètres de redistribution de route RIP et affichez le résumé de redistribution de route

Vous pouvez configurer les paramètres de redistribution de route RIP et afficher le résumé de redistribution de route.

Pour configurer les paramètres de redistribution de route RIP et afficher le résumé de redistribution de route :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **roulage > RIP > Avancé > redistribution de route**.

La page redistribution de route s'affiche.

Les options que vous pouvez sélectionner dans le menu **source** ne comprennent que les routes sources déjà configurées pour la redistribution par RIP. Cela vous permet de configurer une autre route source parmi les routes sources disponibles.

6. Dans le menu **source**, sélectionnez l'un des types de routes sources suivants :

- Connecté Permet de configurer les paramètres des routes connectées.
- Statique Permet de configurer les paramètres des routes statiques.
- **OSPF** : Permet de configurer les paramètres des routes OSPF.

7. Dans le menu **mode de redistribution**, sélectionnez **Activer** ou **désactiver** pour activer ou désactiver le mode de redistribution RIP pour le type de route source sélectionné.

La valeur par défaut est désactiver.

8. Dans le champ **métrique**, spécifiez la valeur métrique des routes redistribuées pour le type de route source sélectionné.

La plage est de 0 à 15. La valeur par défaut est 0, ce qui signifie qu'aucune valeur métrique n'est en vigueur.

9. Dans le champ **liste de distribution**, spécifiez la liste d'accès qui doit filtrer les routes à redistribuer par le protocole de destination.

Seules les routes autorisées sont redistribuées. Si ce champ fait référence à une liste d'accès inexistante, toutes les routes sont autorisées. La plage des ID de liste d'accès est comprise entre 0 et 199. (Pour plus d'informations, consultez la section [Liste de contrôle d'accès](#) à la page 1028.) La valeur par défaut est 0, ce qui signifie qu'aucune liste d'accès n'est en vigueur.

Lorsque vous utilisez une liste d'accès pour le filtrage de route, seuls les champs suivants de la liste d'accès sont utilisés :

- Adresse IP source et masque de réseau
- Adresse IP de destination et masque de réseau
- Action (autoriser ou refuser)

Tous les autres champs (tels que Port source et destination, précedence, ToS, etc.) sont ignorés.

L'adresse IP source est comparée à l'adresse IP de destination de la route. Le masque de réseau IP source dans la règle de liste d'accès est traité comme un masque générique, indiquant quels bits de l'adresse IP source doivent correspondre à l'adresse de destination de la route.

! Remarque: Dans la liste de contrôle d'accès, si vous entrez 1 comme valeur pour le masque de réseau, la liste de contrôle d'accès ignore le bit d'adresse correspondant.

Lorsqu'une règle de liste d'accès comprend une adresse IP de destination et un masque de réseau (une liste d'accès étendue), l'adresse IP de destination est comparée au masque de réseau de la destination de la route. Le masque de réseau de destination dans la liste d'accès sert de masque générique, indiquant quels bits du masque de destination de la route sont significatifs pour l'opération de filtrage.

10. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

11. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 122 : Informations récapitulatives sur la redistribution de route RIP

Champ	Description
Protocole source	Type de route source à redistribuer par le protocole RIP : • Connecté • Statique • OSPF
Mode redistribution	Indique si la route d'un protocole source est redistribuée. Par défaut, la distribution de route est désactivée.
Métrique	Métrique des routes redistribuées pour la route source. Le champ affiche 0 si la mesure n'est pas configurée.
Distribuer la liste	Liste d'accès qui filtre les routes à redistribuer par le protocole de destination. Le champ affiche 0 si aucune ACL n'est configurée à cet effet.

Table 122 : Informations récapitulatives sur la redistribution de route RIP (A continué)

Champ	Description
Correspondance interne	Indique si une route OSPF interne est redistribuée. Par défaut, cette option est activée.
Correspondance type externe 1	Indique si une route OSPF externe de type 1 est redistribuée. Par défaut, cette fonctionnalité est désactivée.
Correspondance type externe 2	Indique si une route OSPF externe de type 2 est redistribuée. Par défaut, cette fonctionnalité est désactivée.
Correspondance type externe NSSA 1	Indique si une route OSPF NSSA de type 1 est redistribuée. Par défaut, cette fonctionnalité est désactivée.
Correspondre au type externe NSSA 2	Indique si une route OSPF NSSA de type 2 est redistribuée. Par défaut, cette fonctionnalité est désactivée.

Découverte de routeurs et annonces de routeurs

Par défaut, une interface de routage n'envoie pas d'annonces de routeur. vous pouvez activer les annonces de routeur pour une interface de routage et configurer le paramètre pour les annonces de routeur.

Pour configurer la découverte de routeurs pour une interface de routage :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > découverte du routeur > Configuration de la découverte du routeur**.

La page Configuration de la découverte du routeur s'affiche.

6. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :

- **1 ou ID d'unité pour un commutateur empilé :**
 - 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
 - **ID d'unité pour un commutateur empilé :** Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
- **VLAN** Seuls les VLAN sont affichés.
- **Tous:** Les interfaces physiques et les VLAN sont affichés, ou pour une pile de commutateurs, les interfaces physiques et les VLAN de tous les commutateurs sont affichés.

7. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :

- Pour afficher ou effacer les statistiques d'une seule interface, cochez la case associée à l'interface ou saisissez le numéro de l'interface dans le champ **aller à l'interface** et cliquez sur le bouton **aller**.
- Pour configurer plusieurs interfaces avec les mêmes paramètres, cochez la case associée à chaque interface.
- Pour configurer toutes les interfaces avec les mêmes paramètres, cochez la case dans la ligne d'en-tête.

8. Dans le menu **mode publicité**, sélectionnez **Activer** ou **désactiver** pour activer ou désactiver la transmission des annonces de routeur sur l'interface.

La valeur par défaut est désactiver.

9. Dans le champ **Advertise Address**, spécifiez l'adresse IPv4 que l'interface doit utiliser pour les annonces de routeur.
10. Dans le champ **intervalle maximum de publicité**, spécifiez la période maximale en secondes autorisée entre les annonces de routeur envoyées depuis l'interface.
Le numéro de port doit être compris entre 4 et 1800. La valeur par défaut est 600.
11. Dans le champ **intervalle minimum de publicité**, spécifiez la période minimale en secondes autorisée entre les annonces de routeur envoyées depuis l'interface.
Le numéro de port doit être compris entre 3 et 1800. Le numéro par défaut est 450.
12. Dans le champ **durée de vie annoncée**, spécifiez la période maximale en secondes pendant laquelle l'adresse annoncée par l'interface est considérée comme une adresse de routeur valide par les hôtes.
Le numéro de port doit être compris entre 4 et 9000. La valeur par défaut est 1800.
13. Dans le champ **niveau de préférence**, spécifiez le niveau de préférence de l'interface du routeur en tant que routeur par défaut par rapport aux autres routeurs du même sous-réseau.
Un nombre plus élevé signifie que l'adresse annoncée reçoit une préférence plus élevée. Le numéro par défaut est 0.
14. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
15. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Virtual Router Redundancy Protocol

Si vous configurez une *route statique* entre un périphérique et un routeur (ou commutateur) qui traite le trafic routé du périphérique, vous introduisez effectivement un point de défaillance unique potentiel dans le réseau. Si le routeur tombe en panne, le périphérique ne peut pas communiquer. Le protocole VRRP (Virtual Router Redundancy Protocol) peut fournir un mécanisme de sauvegarde via l'utilisation d'un routeur principal et d'un routeur secondaire.

Si le routeur principal tombe en panne, VRRP peut laisser le routeur secondaire prendre le relais du routeur principal sans affecter le périphérique qui utilise la route statique. Le périphérique utilise une adresse IP virtuelle reconnue par le routeur secondaire si le routeur principal tombe en panne.

Vous pouvez configurer des ports physiques ou des VLAN routés en tant que ports de routeur VRRP. Les ports qui participent à VRRP utilisent un protocole de sélection qui

détermine quel port fonctionne comme routeur principal. Vous pouvez configurer plusieurs ports sur le commutateur en tant que ports de routeur virtuel. Un seul port peut être visible par le réseau comme plusieurs routeurs virtuels.

Activez VRRP et ajoutez un routeur virtuel principal

Vous pouvez activer VRRP et ajouter un routeur virtuel principal en configurant son ID de routeur virtuel (VRID), en sélectionnant son interface et en définissant son adresse IP principale.

Pour activer VRRP et ajouter un routeur virtuel principal :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.
4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **roulage > VRRP > basique > Configuration VRRP** .
L'écran VRRP Configuration (Configuration IP) s'affiche. La page affiche différentes sections.

6. Sélectionnez un bouton radio mode Admin :
 - Activer. VRRP est activé pour le commutateur.
 - Désactiver : VRRP est désactivé pour le commutateur. Il s'agit de l'option par défaut.
 7. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
 8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.
 9. Dans le champ **VRID**, entrez un nombre compris entre 1 et 255.
Le VRID permet aux routeurs virtuels de communiquer entre eux dans une configuration VRRP. Autrement dit, les routeurs virtuels principal et secondaire doivent avoir le même VRID.
 10. Dans le menu **interface**, sélectionnez l'interface qui doit fonctionner comme routeur virtuel principal.
 11. Dans le champ **adresse IP principale**, entrez l'adresse IP du routeur virtuel principal.
 12. Dans le menu **mode**, sélectionnez si le routeur virtuel est activé :
 - **Actif**. Le routeur virtuel principal est activé.
 - Inactif : Le routeur virtuel principal est configuré mais désactivé.
 13. Cliquez sur le bouton **Add** (Ajouter).
Les paramètres sont enregistrés. Le routeur virtuel principal est ajouté.
 14. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.
- Le tableau suivant décrit les champs en lecture seule de la page.

Champ	Description
Adresse IP de l'interface	Adresse IP associée au profil réseau Cette adresse IP peut être différente de l'adresse IP principale.
Etat	État du routeur virtuel : • Initialisation Le routeur virtuel est en cours d'initialisation. • Maître : Le routeur virtuel a terminé l'initialisation et fonctionne comme routeur principal. • Sauvegarde : Le routeur virtuel a terminé l'initialisation et fonctionne comme routeur secondaire.

Activez VRRP et ajoutez un routeur virtuel principal avec des paramètres améliorés

Vous pouvez activer VRRP et ajouter un routeur virtuel principal en configurant son ID de routeur virtuel (VRID), en sélectionnant son interface et en définissant son adresse IP principale. En outre, vous pouvez configurer plusieurs paramètres améliorés.

Pour activer VRRP et ajouter un routeur virtuel principal avec des paramètres améliorés

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > VRRP > Avancé > Configuration VRRP**.

L'écran VRRP Configuration (Configuration IP) s'affiche. La page affiche différentes sections.

6. Sélectionnez un bouton radio mode Admin :

- Activer. VRRP est activé pour le commutateur.
 - Désactiver : VRRP est désactivé pour le commutateur. Il s'agit de l'option par défaut.
7. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
 8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.
 9. Dans le champ **VRID**, entrez un nombre compris entre 1 et 255.
Le VRID permet aux routeurs virtuels de communiquer entre eux dans une configuration VRRP. Autrement dit, les routeurs virtuels principal et secondaire doivent avoir le même VRID.
 10. Dans le menu **interface**, sélectionnez l'interface qui doit fonctionner comme routeur virtuel principal.
 11. Dans le menu **mode de préemption**, sélectionnez si un routeur virtuel de sauvegarde peut préempter le routeur virtuel principal :
 - Activer. Un routeur VRRP de secours peut préempter le routeur virtuel principal si le routeur de secours a une priorité supérieure à celle du routeur virtuel principal *et si* l'adresse IP dans le champ adresse IP principale (voir ci-dessous) n'est pas l'adresse IP du routeur virtuel principal. La valeur par défaut est Activer.
 - Désactiver : Un routeur virtuel de sauvegarde ne peut pas préempter le routeur virtuel principal.
 12. Dans le menu **Accept mode**, indiquez si le routeur virtuel principal peut accepter les paquets de données :
 - Activer. Le routeur virtuel principal accepte tous les types de paquets de données adressés à l'adresse IP associée au routeur virtuel principal.
 - Désactiver : Le routeur virtuel principal rejette tous les types de paquets de données adressés à l'adresse IP associée au routeur virtuel principal, sauf si l'adresse IP du champ adresse IP principale (voir ci-dessous) est l'adresse IP du routeur virtuel principal. La valeur par défaut est désactiver.
 13. Dans le champ **priorité configurée**, entrez le numéro de priorité que VRRP utilise pour choisir le routeur virtuel principal.
La plage est de 1 à 254. Si l'adresse IP virtuelle est identique à l'adresse IP de l'interface, la priorité est toujours définie sur 254.
 14. Dans le champ **intervalle d'annonce**, entrez le temps, en secondes, entre la transmission des paquets d'annonce par le routeur.
Entrez un nombre compris entre 1 et 255. La valeur par défaut est 1 secondes.
 15. Dans le champ **adresse IP principale**, entrez l'adresse IP du routeur virtuel principal.

16. Dans le menu **Authentication type**, sélectionnez si l'authentification est activée pour le routeur virtuel principal.
 - **Aucun** : Aucune authentification n'est effectuée. Il s'agit de la valeur par défaut.
 - **Tranquillité d'esprit** : L'authentification est effectuée à l'aide d'un mot de passe texte.
17. Si vous sélectionnez **simple** dans le menu **type d'authentification**, entrez un mot de passe dans le champ **données d'authentification**.
18. Dans le menu **Status**, sélectionnez si le routeur virtuel principal est activé :
 - **Actif** : Le routeur virtuel principal est activé.
 - **Inactif** : Le routeur virtuel principal est configuré mais désactivé.
19. Cliquez sur le bouton **Add** (Ajouter).
Les paramètres sont enregistrés. Le routeur virtuel principal est ajouté.
20. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Champ	Description
Priorité opérationnelle	Priorité utilisée pour le processus de sélection VRRP du routeur virtuel principal. Une valeur plus élevée est une priorité plus élevée. Un routeur virtuel principal se voit attribuer une priorité de 0 si informatique ne participe plus au VRRP car un routeur virtuel de sauvegarde a pris le relais. Un routeur virtuel se voit attribuer une priorité de 255 si l'adresse IP de l'interface est identique à l'adresse IP principale.
Adresse IP de l'interface	Adresse IP associée au profil réseau Cette adresse IP peut être différente de l'adresse IP principale.
Propriétaire	Indique si l'adresse IP de l'interface est identique à l'adresse IP principale : • Vrai : L'adresse IP de l'interface est identique à l'adresse IP principale. Dans un processus de sélection VRRP, si le routeur virtuel est actif et que son adresse IP d'interface est identique à l'adresse IP principale, informatique remporte toujours une sélection pour le routeur virtuel principal. • Faux : L'adresse IP de l'interface est différente de l'adresse IP principale.
Adresse VMAC	Adresse MAC virtuelle associée au routeur virtuel. Cette adresse MAC se compose d'un identifiant unique de 24 bits, de la constante de 16 bits identifiant le bloc d'adresse VRRP et du VRID de 8 bits.
Etat	État du routeur virtuel : • Initialisation : Le routeur virtuel est en cours d'initialisation. • Maître : Le routeur virtuel a terminé l'initialisation et fonctionne comme routeur principal. • Sauvegarde : Le routeur virtuel a terminé l'initialisation et fonctionne comme routeur secondaire.

Modifiez les paramètres d'un routeur virtuel principal

Vous pouvez modifier les paramètres d'un routeur virtuel principal existant.

Pour modifier les paramètres d'un routeur virtuel principal :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > VRRP > Avancé > Configuration VRRP**.

L'écran VRRP Configuration (Configuration IP) s'affiche. La page affiche différentes sections.

6. Cochez la case correspondant à l'ID VRRP (VRID), qui identifie le routeur virtuel principal.

7. Modifiez les paramètres en fonction de vos besoins.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Activez VRRP et ajoutez un routeur virtuel principal avec des paramètres améliorés](#) à la page 593.

8. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimez un routeur virtuel principal

Vous pouvez supprimer un routeur virtuel principal dont vous n'avez plus besoin.

Pour supprimer un routeur virtuel principal :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur principale à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > VRRP > Avancé > Configuration VRRP**.

L'écran VRRP Configuration (Configuration IP) s'affiche. La page affiche différentes sections.

6. Cochez la case correspondant à l'ID VRRP (VRID), qui identifie le routeur virtuel principal.

7. Cliquez sur le bouton **Supprimer**.

Les paramètres sont enregistrés. Le routeur virtuel principal est supprimé.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez un routeur virtuel secondaire

Un routeur virtuel auquel est attribuée une adresse IP secondaire VRRP peut devenir le nouveau routeur virtuel principal si le routeur virtuel d'origine tombe en panne. Les routeurs virtuels principal et secondaire doivent avoir le même ID de routeur virtuel (VRID).

Pour configurer un routeur virtuel secondaire :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **roulage > VRRP > Avancé > Configuration de l'adresse IP secondaire VRRP**.

La page Configuration de l'adresse IP secondaire VRRP s'affiche. La page affiche différentes sections.

6. Dans le menu **interface VRRP**, sélectionnez l'interface VRRP qui doit fonctionner comme routeur virtuel secondaire.
7. Dans le menu **VRRP ID**, sélectionnez le VRID attribué au routeur virtuel secondaire.
8. Dans le champ **adresse IP secondaire**, entrez l'adresse IP du routeur virtuel secondaire.
Cette adresse doit faire partie d'un sous-réseau d'adresses IP sur l'interface.
Les champs adresse IP principale affichent l'adresse IP attribuée au routeur virtuel principal avec le même VRID.
9. Cliquez sur le bouton **Add** (Ajouter).
Les paramètres sont enregistrés. Le routeur virtuel secondaire est ajouté.
10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Modifiez l'adresse IP d'un routeur virtuel secondaire

Vous pouvez modifier l'adresse IP d'un routeur virtuel secondaire existant.

Pour modifier l'adresse IP d'un routeur virtuel secondaire :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **roulage > VRRP > Avancé > Configuration de l'adresse IP secondaire VRRP** .
La page Configuration de l'adresse IP secondaire VRRP s'affiche. La page affiche différentes sections.
6. Dans le menu **interface VRRP**, sélectionnez l'interface VRRP.
7. Dans le menu **VRRP ID**, sélectionnez le VRID.
8. Cochez la case correspondant à l'adresse IP secondaire.
9. Dans le champ **Trusted IP Address** (Adresse IP de confiance), saisissez l'adresse IP.
10. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
11. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimez un routeur virtuel secondaire

Vous pouvez supprimer un routeur virtuel secondaire dont vous n'avez plus besoin.

Pour supprimer un routeur virtuel secondaire :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > VRRP > Avancé > Configuration de l'adresse IP secondaire VRRP**.

La page Configuration de l'adresse IP secondaire VRRP s'affiche. La page affiche différentes sections.

6. Dans le menu **interface VRRP**, sélectionnez l'interface VRRP.
7. Dans le menu **VRRP ID**, sélectionnez le VRID.
8. Cochez la case correspondant à l'adresse IP secondaire.
9. Cliquez sur le bouton **Supprimer**.

Les paramètres sont enregistrés. Le routeur virtuel secondaire est supprimé.

10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurer le suivi d'interface VRRP et le suivi d'itinéraire

Vous pouvez laisser VRRP suivre des interfaces et des routes spécifiques et laisser VRRP déterminer si elles peuvent être atteintes. Si une interface ou une route suivie n'est pas accessible, VRRP peut laisser un routeur secondaire prendre le relais.

Pour configurer le suivi d'interface VRRP et le suivi d'itinéraire :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > VRRP > Avancé > Configuration du suivi VRRP**.

La page Configuration du suivi VRRP s'affiche. La page affiche différentes sections.

6. Dans le menu **interface VRRP**, sélectionnez l'interface VRRP que vous souhaitez suivre.
7. Dans le menu **ID VRRP**, sélectionnez l>ID de routeur virtuel (VRID) que vous souhaitez suivre.
8. Dans la section Configuration de l'interface de suivi VRRP, configurez les paramètres suivants :

- Dans le menu **interface suivie**, sélectionnez l'interface de routage à suivre.

Le menu affiche toutes les interfaces de routage qui ne sont pas encore suivies pour la combinaison interface VRRP et ID VRRP sélectionnée. Les interfaces de bouclage et les tunnels qui ne peuvent pas être suivis ne sont pas affichés.

- Dans le champ **diminution de priorité**, entrez une valeur de diminution de priorité pour l'interface suivie.

Si l'interface ne peut pas être atteinte, sa priorité VRRP est diminuée de la valeur que vous entrez. La plage est de 1 à 254. Le numéro par défaut est 10.

Le champ Etat de l'interface suivie s'affiche si l'interface peut être atteinte.

9. Dans la section Configuration de la route de suivi VRRP, configurez les paramètres suivants :

- Dans le champ **préfixe de la route suivie**, entrez le préfixe de la route à suivre.
- Dans le champ **longueur du préfixe de la route suivie**, entrez la longueur du préfixe de la route à suivre.
- Dans le champ **diminution de priorité**, entrez une valeur de diminution de priorité pour l'itinéraire suivi.

Si la route ne peut pas être atteinte, sa priorité VRRP est diminuée de la valeur que vous entrez.

La plage est de 1 à 254. Le numéro par défaut est 10.

Le champ accessible indique si l'itinéraire suivi peut être atteint.

10. Cliquez sur le bouton **Add** (Ajouter).

Les paramètres sont enregistrés. La configuration de suivi est ajoutée.

11. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Afficher les statistiques VRRP

Si VRRP est activé, vous pouvez afficher les statistiques VRRP globales et les statistiques pour chaque ID VRRP.

Pour afficher les statistiques VRRP :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > Avancé > statistiques VRRP**.

La page statistiques VRRP s'affiche. La page affiche différentes sections.

6. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

Le tableau suivant décrit les champs en lecture seule de la page.

Champ	Description
Statistiques globales	
Erreurs de somme de contrôle du routeur	Nombre de paquets VRRP reçus avec une valeur de somme de contrôle VRRP non valide
Erreurs de version du routeur	Nombre de paquets VRRP reçus avec un numéro de version inconnu ou non pris en charge
Erreurs VRID du routeur	Nombre de paquets VRRP reçus avec un VRID non valide
Statistiques	
ID VRRP	L>ID VRRP (VRID)
Interface	Interface configurée en tant que routeur virtuel
Durée de fonctionnement	Temps, en jours, heures, minutes et secondes, écoulé depuis que le routeur virtuel est passé à l'état initialisé
État transféré vers maître	Nombre de fois que l'état du routeur virtuel est passé à l'état principal
Annonce reçue	Nombre d'annonces VRRP reçues par le routeur virtuel
Erreurs d'intervalle d'annonce	Nombre de paquets d'annonce VRRP reçus pour lesquels l'intervalle d'annonce était différent de celui configuré pour le routeur virtuel
Echec de l'authentification	Nombre de paquets VRRP reçus qui n'ont pas réussi le contrôle d'authentification

(A continué)

Champ	Description
Erreurs TTL IP	Nombre de paquets VRRP reçus par le routeur virtuel avec une valeur de durée de vie (TTL) différente de 255
Paquets de priorité zéro reçus	Nombre de paquets VRRP reçus par le routeur virtuel avec une priorité de 0
Paquets de priorité zéro envoyés	Nombre de paquets VRRP envoyés par le routeur virtuel avec une priorité de 0
Paquets de type non valides reçus	Nombre de paquets VRRP reçus par le routeur virtuel avec un type non valide
Erreurs de liste d'adresses	Nombre de paquets reçus pour lesquels la liste d'adresses ne correspond pas à la liste configurée localement pour le routeur virtuel
Type d'authentification invalide.	Nombre de paquets reçus avec un type d'authentification inconnu
Type d'authentification non concordant	Nombre de paquets reçus avec un type d'authentification différent de la méthode d'authentification configurée localement
Erreurs de longueur de paquet	Nombre total de paquets reçus avec une longueur de paquet inférieure à la longueur de l'en-tête VRRP

6

Configurez OSPF et OSPFv3

Ce chapitre aborde les sujets suivants :

- Ouvrez d'abord le chemin le plus court
- Open Shortest Path First version 3

❗ **Remarque:** Dans ce chapitre, Open Shortes path First (OSPF) fait référence à OSPF version 2 (OSPFv2). OSPFv3 fait référence à OSPF version 3.

Ouvrez d'abord le chemin le plus court

Open Shortest Path First (OSPF) permet au commutateur de déterminer la meilleure route (la plus courte) vers une destination. Pour les grands réseaux, OSPF est généralement utilisé de préférence au protocole RIP (Routing Information Protocol).

Si vous gérez un réseau volumineux ou complexe, OSPF offre plusieurs avantages :

- **Moins de trafic réseau :**

- Les mises à jour de la table de routage sont envoyées uniquement lorsqu'une modification se produit
- Seule la partie de la table qui change est envoyée
- Les mises à jour sont envoyées à une adresse de multidiffusion plutôt qu'à une adresse de diffusion

- **Gestion hiérarchique :**

La gestion hiérarchique permet de subdiviser le réseau.

Le niveau supérieur de la hiérarchie d'un réseau OSPF est appelé système autonome (AS) ou domaine de routage. Il s'agit d'un ensemble de réseaux avec une stratégie d'administration et de routage commune. L'AS est divisé en zones :

- **Intra-zone** : Le routage intra-zone est utilisé lorsqu'une adresse source et une adresse de destination se trouvent dans la même zone.
- **Inter-zone** : Le routage inter-zone sur un backbone OSPF est utilisé lorsqu'une adresse source et une adresse de destination *ne* se trouvent *pas* dans la même zone. Un routeur inter-zone communique avec des routeurs de bordure dans chacune des zones auxquelles informatique fournit une connectivité.

Si vous activez OSPF sur le commutateur, informatique détermine la meilleure route en utilisant le coût attribué et le type de route OSPF. Si plusieurs types d'itinéraire sont présents, le commutateur sélectionne un itinéraire en fonction de l'ordre de préférence suivant :

1. Route intra-zone
2. Route inter-zone
3. Routage externe de type 1 : Le routage est externe à l'AS
4. Routage externe de type 2 : La route est apprise à partir d'autres protocoles tels que RIP

Activer OSPF

Avant que OSPF ne devienne opérationnel, vous devez activer le mode administratif pour le routage IPv4 sur le commutateur (voir [Configuration des paramètres IP de routage à la page 307](#) à la page 532).

Pour activer OSPF :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > OSPF > basique > Configuration OSPF** .

L'écran OSPF Configuration (Configuration IP) s'affiche.

6. Sélectionnez un bouton radio mode Admin :

- Activer. OSPF est activé pour le commutateur. Il s'agit de l'option par défaut.
- Désactiver : OSPF est désactivé pour le commutateur.

Le champ ID routeur affiche le nombre 32 bits au format décimal à points. Ce numéro identifie de manière unique le commutateur au sein du système autonome (AS).

Pour modifier l'ID du routeur, vous devez d'abord désactiver OSPF. Après avoir défini un nouvel ID de routeur, vous devez réactiver OSPF pour que la modification prenne effet. La valeur par défaut est 0,0.0,0, bien qu'il ne s'agisse pas d'un ID de routeur valide.

7. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez l'annonce de route par défaut OSPF

Qu'une route par défaut existe ou non dans la table de routage, vous pouvez configurer une route par défaut pour les annonces OSPF, y compris une valeur de métrique et un type de métrique.

Pour configurer l'annonce de route par défaut OSPF :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **routage > OSPF > Avancé > Configuration OSPF** .
L'écran OSPF Configuration (Configuration IP) s'affiche. La page affiche différentes sections.
6. Accédez à la section Configuration d'annonce de route par défaut.
7. Sélectionnez un bouton radio d'origine des informations par défaut :
 - Activer. OSPF génère une route par défaut pour la publicité LSA externe. Cette route est au format X.X.X.X/X.X.X.X.
 - Désactiver : OSPF ne génère pas de route par défaut pour la publicité LSA externe. Il s'agit de l'option par défaut.
8. Sélectionnez un bouton radio toujours :
 - Vrai OSPF émet une route par défaut, qu'une route par défaut existe ou non.
 - Faux OSPF émet une route par défaut uniquement si une route par défaut se trouve déjà dans la table de routage du commutateur.
9. Dans le champ **métrique**, définissez la valeur métrique de l'itinéraire par défaut.
La valeur est comprise entre 0 et 16777214. Le numéro par défaut est 0.
10. Bouton radio sélectionner un champ type d'audit :
 - **Externe type 1** : Cette mesure est calculée en ajoutant le coût OSPF interne au coût redistribué externe.
 - **Externe type 2** : Cette métrique est calculée en utilisant uniquement le coût redistribué externe. Il s'agit de la valeur par défaut.
11. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
12. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez les paramètres OSPF globaux

Vous pouvez configurer les paramètres OSPF qui s'appliquent globalement aux processus OSPF sur le commutateur.

Pour configurer les paramètres OSPF globaux :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > OSPF > Avancé > Configuration OSPF**.

L'écran OSPF Configuration (Configuration IP) s'affiche. La page affiche différentes sections.

6. Accédez à la section Configuration OSPF.

7. Dans le champ **Router ID (ID du routeur)**, entrez le nombre de 32 bits au format décimal à points qui identifie de manière unique le routeur au sein du système autonome (AS).

Pour modifier l'ID du routeur, vous devez d'abord désactiver OSPF. Après avoir défini un nouvel ID de routeur, vous devez réactiver OSPF pour que la modification prenne effet. La valeur par défaut est 0,0.0,0, bien qu'il ne s'agisse pas d'un ID de routeur valide.

8. Sélectionnez un bouton radio mode Admin :

- Activer. OSPF est activé pour le commutateur. Il s'agit de l'option par défaut.
- Désactiver : OSPF est désactivé pour le commutateur.

Avant que OSPF ne devienne opérationnel, vous devez activer le mode d'administration pour le routage IPv4 sur le commutateur (voir [Gérer les paramètres de routage IPv4 globaux](#) à la page 532).

9. Dans le menu **compatibilité RFC 1583**, sélectionnez la manière dont le commutateur définit automatiquement les règles de préférence pour les annonces d'état de liens (LSA) si plusieurs LSA AS-externes annoncent la même destination :
 - Activer. Les règles de préférence empêchent les boucles de routage lorsque les AS-External-LSA de la même destination proviennent de zones différentes. Tous les routeurs ou commutateurs du domaine OSPF doivent être configurés de la même manière. Activer est le paramètre par défaut.

Pour plus d'informations, reportez-vous à la section 16.4.1 de la norme OSPF-2 (RFC 2328) : <https://datatracker.ietf.org/doc/html/rfc2328>
 - Désactiver : Si tous les routeurs OSPF sont capables de fonctionner conformément à la norme décrite dans la RFC 2328, désactivez la compatibilité RFC 1583.
10. Dans le menu **opaque LSA Status**, sélectionnez la manière dont le commutateur traite les LSA opaques :
 - Activer. Le commutateur stocke les LSA opaques. Un LSA opaque est utilisé pour inonder des informations définies par l'utilisateur dans un domaine de routeur OSPF.
 - Désactiver : Le commutateur ne stocke pas de LSA opaques.
11. Dans le champ **intervalle de débordement de sortie**, définissez le nombre de secondes que OSPF doit attendre avant de quitter un état de débordement.

Lorsque le nombre de LSA externes autres que ceux par défaut dépasse une limite, le commutateur entre dans un état de dépassement dans lequel OSPF ne peut pas émettre de LSA externes autres que ceux par défaut. (Pour plus d'informations, voir RFC 1765.)

Si le nombre de secondes est 0 (paramètre par défaut), OSPF ne quitte pas l'état de débordement tant que vous n'avez pas désactivé et réactivé OSPF. La valeur maximale possible est de 2 147 483 647 secondes.
12. Dans le champ **délai SPF**, définissez combien de secondes OSPF doit attendre avant de commencer un nouveau calcul SPF (Shortest Path First).

Le délai SPF est le nombre de secondes entre le moment où OSPF reçoit une modification de topologie et le début du calcul SPF suivant. Le délai peut être de 0 à 65535 secondes. La valeur par défaut est de 5 secondes. Une valeur de 0 signifie qu'il n'y a pas de délai : le calcul SPF est lancé dès qu'un changement de topologie se produit.
13. Dans le champ **temps de maintien SPF**, définissez le nombre de secondes que OSPF doit attendre entre deux calculs SPF consécutifs.

Le temps de maintien SPF est le temps minimum en secondes entre deux calculs SPF consécutifs. Le temps de maintien peut être compris entre 0 et 65 535 secondes. La valeur par défaut est 10 secondes. Une valeur de 0 signifie qu'il n'y a pas de délai : deux calculs SPF peuvent être effectués, l'un immédiatement après l'autre.

14. Dans le champ **External LSDB Limit**, définissez la limite de la base de données d'état de liens externe (LSDB) pour OSPF.

Lorsque le nombre d'AS-External-LSA autres que celui par défaut dans la base de données d'état de liaison d'un routeur atteint la limite de la LSDB externe, le routeur passe en état de dépassement de capacité. Le routeur ne peut pas contenir plus de LSA AS-External-LSA sans valeur par défaut que le nombre maximal que la carte LSDB externe peut contenir. La limite de la carte LSDB externe doit être définie de manière identique dans tous les routeurs rattachés au backbone OSPF ou à toute zone OSPF normale. La limite peut être comprise entre -1 et 2147483647. Le paramètre par défaut est -1, ce qui indique qu'il n'y a pas de limite.

15. Dans le champ **mesure par défaut**, définissez la mesure par défaut des routes redistribuées.

La plage est de 1 à 16777214. Le numéro par défaut est 0.

16. Dans le champ **nombre maximal de chemins**, définissez le nombre de chemins qu'OSPF peut signaler pour une destination.

La plage est de 1 à 16. Le numéro par défaut est 4.

17. Dans le champ **bande passante de référence autocost**, définissez la bande passante qui contrôle la façon dont OSPF calcule le coût de la liaison.

Définissez la bande passante de référence en mégabits par seconde. À moins qu'un coût de liaison ne soit configuré, le coût de liaison est calculé en divisant la largeur de bande de référence par la largeur de bande de l'interface. La plage est de 1 à 4294967. Le numéro par défaut est 100.

18. Dans le menu **Paramètres passifs par défaut**, sélectionnez la manière dont le paramètre de mode passif global pour toutes les interfaces OSPF est configuré :

- Activer. L'activation du mode passif remplace globalement tout paramètre de mode passif au niveau de l'interface. OSPF ne forme pas de contiguïtés sur les interfaces passives, mais annonce les réseaux attachés comme des réseaux stub.
- Désactiver : La valeur par défaut est désactiver.

19. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

20. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Champ	Description
Mode ASBR	Le routeur est un routeur de limite de système autonome (ASBR) si informatique est configuré pour redistribuer les routes à partir d'un autre protocole, ou si informatique est configuré pour émettre un LSA externe annonçant la route par défaut.
Etat ABR	Le routeur est un routeur de bordure de zone (ABR) si informatique possède des interfaces non virtuelles actives dans deux zones OSPF ou plus.
Décompte LSA externe	Nombre d'annonces d'état de lien (LSA) externes (LS type 5) dans la base de données d'état de lien.
Somme de contrôle LSA externe	Somme des sommes de contrôle LS des LSA externes contenues dans la base de données d'état des liens. Vous pouvez utiliser cette somme pour déterminer s'il y a eu un changement dans la base de données d'état des liaisons d'un commutateur ou d'un routeur, et pour comparer les bases de données d'état des liaisons de deux unités. Cette valeur est en hexadécimal.
AS_OPAQUE LSA COUNT	Nombre de LSA opaques avec étendue d'inondation à l'échelle du domaine.
AS_OPAQUE LSA CHECKSUM	Somme des sommes de contrôle LS des LSA opaques avec une étendue d'inondation à l'échelle du domaine. Vous pouvez utiliser cette somme pour déterminer s'il y a eu un changement dans la base de données d'état des liaisons d'un commutateur ou d'un routeur, et pour comparer les bases de données d'état des liaisons de deux unités.
De nouveaux LSA ont été créés	Nombre de LSA émis par le commutateur. Dans toute zone OSPF, un routeur (ou dans ce cas, un commutateur) émet plusieurs LSA. Chaque routeur émet un routeur-LSA. Si le routeur est également le routeur désigné pour l'un des réseaux de la zone, informatique émet des LSA réseau pour ces réseaux.
LSA reçus	Nombre de LSA reçus pour les nouvelles instanciations. Ce nombre n'inclut pas les nouvelles instanciations de LSA auto-initiées.

Ajoutez ou supprimez un ID de zone commune OSPF

Une zone commune OSPF se compose d'un groupe de périphériques partageant le même ID de zone.

Pour ajouter ou supprimer un ID de zone commune OSPF :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > OSPF > Avancé > Configuration de la zone commune** .

La page Configuration de la zone commune OSPF s'affiche.

6. Dans le champ **ID de zone**, saisissez un ID de zone OSPF.

Un ID de zone est un entier de 32 bits au format décimal à points qui identifie de manière unique la zone à laquelle une interface est connectée.

7. Effectuez l'une des actions suivantes :

- Ajouter Cliquez sur le bouton **Add** (Ajouter).

L'ID de zone est ajouté.

- Supprimer Cliquez sur le bouton **Supprimer**.

L'ID de zone est supprimé.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Champ	Description
Routage externe	Une définition des capacités du commutateur pour la zone, y compris si oui ou non des AS-externes-LSA sont inondés dans ou dans toute la zone. Si la zone est une zone de segment d'accroche, l'une des fonctions de routage externe suivantes peut s'afficher : • Importer des LSA externes : Importe et propage les LSA externes. • N° d'importation LSA : N'importe pas et ne propage pas les LSA externes. Si la zone n'est pas une zone de segment d'accroche, la seule option est Importer aucun LSA.
SPF fonctionne	Nombre de fois que la table de route intra-zone a été calculée à l'aide de la base de données d'état des liens de cette zone. (Ceci est généralement calculé en utilisant l'algorithme de Dijkstra.)
Nombre de routeurs de bordure de zone	Le nombre total de routeurs de bordure de zone qui sont accessibles à nouveau dans cette zone. Il est initialement nul, et est calculé à chaque passe SPF.
Décompte LSA zone	Nombre d'annonces d'état de lien dans la base de données d'état de lien de cette zone, à l'exclusion DES LSA externes.
Somme de contrôle LSA zone	Somme non signée de 32 bits de la somme de contrôle d'annonce d'état de lien contenue dans la base de données d'état de lien de cette zone. Cette somme exclut les annonces d'état de lien externes (LSA type 5). Vous pouvez utiliser la somme pour déterminer si une modification s'est produite dans la base de données d'état de liaison du commutateur et pour comparer la base de données d'état de liaison de deux unités.
Longueur de la liste des inondations	Le nombre de LSA figurant sur la liste des inondations de cette zone.
Importer les LSA récapitulatifs	Récapitulatif des LSA importés dans cette zone.

Ajoutez une zone de stub OSPF

Une zone de stub est une zone contrôlée qui n'autorise pas les routes externes provenant de l'extérieur du réseau OSPF.

Pour ajouter une zone de stub OSPF :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > OSPF > Avancé > Configuration de la zone de tronçon**.

La page Configuration de la zone de stub OSPF s'affiche.

6. Dans le champ **ID de zone**, saisissez un ID de zone OSPF.

Un ID de zone est un entier de 32 bits au format décimal à points qui identifie de manière unique la zone à laquelle une interface est connectée.

7. Dans le menu **Import Summary LSA**, sélectionnez si les LSA récapitulatifs sont importés :

- Activer. Les LSA récapitulatifs sont importés dans des zones de stub.
- Désactiver : Les LSA récapitulatifs ne sont pas importés dans les zones de stub.

8. Dans le champ **coût par défaut**, entrez la valeur métrique qui doit être appliquée pour la route par défaut annoncée à la zone de segment d'accroche.

La plage est de 1 à 16 777 215.

9. Cliquez sur le bouton **Add** (Ajouter).

La zone est ajoutée en tant que zone de segment d'accroche.

10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Champ	Description
SPF fonctionne	Nombre de fois que la table de route intra-zone a été calculée à l'aide de la base de données d'état des liens de cette zone. (Ceci est généralement calculé en utilisant l'algorithme de Dijkstra.)
Nombre de routeurs de bordure de zone	Nombre total de routeurs de bordure de zone accessibles dans cette zone. Il est initialement nul, et est calculé à chaque passe SPF.
Décompte LSA zone	Nombre d'annonces d'état de lien dans la base de données d'état de lien de cette zone, à l'exclusion DES LSA externes.
Somme de contrôle LSA zone	Somme non signée de 32 bits de la somme de contrôle d'annonce d'état de lien contenue dans la base de données d'état de lien de cette zone. Cette somme exclut les annonces d'état de lien externes (LSA type 5). Vous pouvez utiliser la somme pour déterminer si une modification s'est produite dans la base de données d'état de liaison du commutateur et pour comparer la base de données d'état de liaison de deux unités.
Type de service	ToS normal associé à la métrique segment d'accroche.

Ajoutez une zone NSSA OSPF

La zone OSPF Not-SO-stubby (NSSA) peut recevoir des routes externes (LSA de type 7) et apprendre des routes à partir d'autres protocoles tels que le protocole RIP et transférer ces routes vers d'autres zones. Vous pouvez choisir si les LSA récapitulatifs (LSA de type 3) peuvent être importés dans des zones de stub.

Pour ajouter une zone NSSA OSPF :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > OSPF > Avancé > Configuration de zone NSSA**.

La page Configuration de zone NSSA OSPF s'affiche.

6. Dans le champ **ID de zone**, saisissez un ID de zone OSPF.

Un ID de zone est un entier de 32 bits au format décimal à points qui identifie de manière unique la zone à laquelle une interface est connectée.

7. Dans le menu **Import Summary LSA**, sélectionnez si les LSA récapitulatifs sont importés :

- Activer. Les LSA récapitulatifs sont importés dans des zones de stub.
- Désactiver : Les LSA récapitulatifs ne sont pas importés dans les zones de stub.

8. Les options de la section Default information Origin du tableau vous permettent de configurer le commutateur pour annoncer une route par défaut dans le NSSA lorsque l'importation des LSA récapitulatifs est désactivée :

- a. Dans le menu **mode Admin**, sélectionnez **Activer** pour laisser le commutateur annoncer une route par défaut ou **désactiver** pour empêcher le commutateur de le faire.

- b. Dans le champ **valeur métrique**, définissez la valeur métrique de la route par défaut.

La plage est de 1 à 16777214.

- c. Dans le menu **type de métrique**, sélectionnez le type de métrique à utiliser dans l'itinéraire par défaut :

- **Coût comparable** : Métriques externes de type 1 comparables à la métrique OSPF
- **Coût non comparable** : Métriques externes de type 2 supposées supérieures au coût de la métrique OSPF.

9. Dans le menu **rôle du traducteur**, sélectionnez le rôle du NSSA :

- **Toujours**: Le commutateur assume le rôle de traducteur lorsque informatique devient un routeur de frontière.
- **Candidat** : Le commutateur participe au processus d'élection du traducteur lorsque informatique atteint l'état de routeur de frontière.

10. Dans le champ **intervalle de stabilité du traducteur**, entrez la période pendant laquelle le commutateur étend son rôle de traducteur après qu'un autre périphérique devient le traducteur.

La plage est de 0 à 3600 secondes.

11. Dans le menu **mode redistribution**, sélectionnez si les routes externes apprises sont redistribuées :

- Activer. L'ABR de la NSSA distribue les routes externes apprises à la NSSA.
- Désactiver : L'ABR de la NSSA ne distribue pas les routes externes apprises à la NSSA.

12. Cliquez sur le bouton **Add** (Ajouter).

La zone est ajoutée en tant que zone NSSA.

13. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Champ	Description
SPF fonctionne	Nombre de fois que la table de route intra-zone a été calculée à l'aide de la base de données d'état des liens de cette zone. (Ceci est généralement calculé en utilisant l'algorithme de Dijkstra.)
Nombre de routeurs de bordure de zone	Nombre total de routeurs de bordure de zone accessibles dans cette zone. Il est initialement nul, et est calculé à chaque passe SPF.
Décompte LSA zone	Nombre d'annonces d'état de lien dans la base de données d'état de lien de cette zone, à l'exclusion DES LSA externes.
Somme de contrôle LSA zone	Somme non signée de 32 bits de la somme de contrôle d'annonce d'état de lien contenue dans la base de données d'état de lien de cette zone. Cette somme exclut les annonces d'état de lien externes (type 5). Vous pouvez utiliser la somme pour déterminer si une modification s'est produite dans la base de données d'état de liaison du commutateur et pour comparer la base de données d'état de liaison de deux unités.
Etat du traducteur	Ce champ indique si et comment le routeur de frontière NSSA convertit les LSA de type 7 en LSA de type 5 : • Sous tension Le rôle de traducteur du routeur de frontière NSSA est défini sur toujours. • Élus : Le routeur de frontière NSSA candidat traduit les LSA de type 7 en LSA de type 5. • Désactivé : Le routeur de frontière NSSA candidat ne traduit pas les LSA de type 7 en LSA de type 5.

Ajoutez une plage de zones OSPF

Vous ajoutez une plage de zones OSPF en définissant un ID de zone avec une plage d'adresses (une adresse IP avec un masque de sous-réseau). Vous définissez ensuite également les LSA associés à la zone et si la plage d'adresses est annoncée en dehors de la zone.

Vous pouvez associer une plage de zones OSPF à une zone commune (voir [Ajoutez ou supprimez un ID de zone commune OSPF](#) à la page 614), une zone de stub (voir [Ajoutez une zone de stub OSPF](#) à la page 616) ou une zone NSSA (voir [Ajoutez une zone NSSA OSPF](#) à la page 618).

Pour ajouter une plage de zones OSPF :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > OSPF > Avancé > Configuration de la plage de zones**.

La page Configuration de la plage de zones OSPF s'affiche.

6. Dans le champ **ID de zone**, saisissez un ID de zone OSPF.

Un ID de zone est un entier de 32 bits au format décimal à points qui identifie de manière unique la zone à laquelle une interface est connectée.

7. Dans le champ **adresse IP**, entrez l'adresse IP de la plage d'adresses.
8. Dans le champ **masque de sous-réseau**, entrez le masque de sous-réseau de la plage d'adresses.
9. Dans le menu **LSDB type**, sélectionnez le type d'annonces d'état de liaison (LSA) qui doit être associé à l'ID de zone et à la plage d'adresses.
 - **Résumé du réseau** : Le commutateur génère des LSA de résumé du réseau (LSA de type 3) pour la zone. Il s'agit de l'option par défaut.
 - **NSSA externe** : Le commutateur génère des LSA externes NSSA (LSA de type 7) pour la zone. Ces types de LSA fournissent plus d'informations.
10. Dans le menu **annoncer**, sélectionnez si la plage d'adresses est annoncée en dehors de la zone :
 - Activer. La plage d'adresses est annoncée en dehors de la zone via les LSA de résumé du réseau. Il s'agit de l'option par défaut.
 - Désactiver : La plage d'adresses n'est pas annoncée en dehors de la zone.
11. Cliquez sur le bouton **Add** (Ajouter).

L'ID OSPF et la plage de zones sont ajoutés.
12. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez une interface OSPF

Vous pouvez configurer une ou plusieurs interfaces OSPF, qui sont connectées à des zones OSPF via des connexions point à point ou de diffusion.

Pour configurer une interface OSPF :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > OSPF > Avancé > statistiques d'interface**.

La page statistiques de l'interface OSPF s'affiche.

6. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :

- **1 ou ID d'unité pour un commutateur empilé :**
 - 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
 - **ID d'unité pour un commutateur empilé :** Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
- **VLAN** Seuls les VLAN sont affichés.
- **Tous:** Les interfaces physiques et les VLAN sont affichés, ou pour une pile de commutateurs, les interfaces physiques et les VLAN de tous les commutateurs sont affichés.

7. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :

- Pour configurer une interface ou un VLAN unique, cochez la case associée à l'interface ou au VLAN, ou tapez le numéro de l'interface ou du VLAN dans le champ **aller à l'interface** et cliquez sur le bouton **aller**.
- Pour configurer plusieurs interfaces ou VLAN avec les mêmes paramètres, cochez la case associée à chaque interface ou VLAN.

8. Dans le champ **ID de zone**, saisissez un ID de zone OSPF.

Un ID de zone est un entier de 32 bits au format décimal à points qui identifie de manière unique la zone à laquelle une interface est connectée.

9. Sélectionnez un bouton radio mode Admin :

- Activer. OSPF est activé pour l'interface.
- Désactiver : OSPF est désactivé pour l'interface. Il s'agit de l'option par défaut.

OSPF peut devenir opérationnel sur l'interface uniquement si l'interface est configurée avec une adresse IP et un masque de sous-réseau (voir [Configurer les interfaces de routage IPv4](#) à la page 538).

Vous pouvez configurer les paramètres OSPF sans activer OSPF sur l'interface, mais la modification ne prend effet que lorsque vous activez OSPF sur l'interface. Les champs suivants s'affichent uniquement si vous activez OSPF sur l'interface :

État, routeur désigné, routeur désigné de sauvegarde, nombre d'événements de liaison, LSA de liaison locale et somme de contrôle LSA de liaison locale.

10. Dans le champ **priorité du routeur**, entrez la priorité OSPF de l'interface.

Il s'agit d'un nombre compris entre 0 et 255. La valeur par défaut est 1, qui est la priorité la plus élevée du routeur. La valeur 0 indique que le routeur n'est pas éligible pour devenir le routeur désigné sur ce réseau.

11. Dans le champ **intervalle de retransmission**, entrez le nombre de secondes entre les annonces d'état de liaison pour les contiguïtés, c'est-à-dire pour les périphériques voisins qui forment une contiguïté OSPF avec l'interface.

L'intervalle est également utilisé lors de la retransmission de descriptions de base de données et de paquets de demande d'état de liens. La valeur de l'intervalle est comprise entre 1 et 3600 secondes (1 heure). La valeur par défaut est de 5 secondes.

12. Dans le champ **Hello Interval**, entrez l'intervalle Hello OSPF de l'interface.

Cet intervalle doit être le même pour tous les routeurs et commutateurs du réseau. L'intervalle est compris entre 1 et 65 535 secondes. La valeur par défaut est 10 secondes.

13. Dans le champ **intervalle mort**, entrez le nombre de secondes pendant lesquelles l'interface attend les paquets Hello d'un voisin avant de déterminer que ce voisin est en panne.

Cet intervalle doit être le même pour tous les routeurs et commutateurs du réseau. Cet intervalle doit être un multiple de l'intervalle Hello. L'intervalle est compris entre 1 et 65 535. La valeur par défaut est de 40 secondes. (L'intervalle Hello par défaut est de 10 secondes.)

14. Dans le champ **lfransit Delay Interval**, entrez le nombre estimé de secondes nécessaires pour transmettre un paquet de mise à jour de l'état de la liaison sur l'interface.

L'intervalle est compris entre 1 et 3600 secondes (1 heure). La valeur par défaut est 1 seconde.

15. Dans le menu **ignorer MTU**, sélectionnez si la détection de discordance MTU OSPF est désactivée :

- Activer. La détection des discordances MTU OSPF est *désactivée* sur les paquets de description de base de données entrants. La valeur par défaut est Disable (désactiver) (la détection des discordances MTU est activée).
 - Désactiver : La détection des discordances MTU OSPF est *activée* sur les paquets de description de base de données entrants. Il s'agit de l'option par défaut.
16. Dans le menu **mode passif**, sélectionnez si l'interface ne forme pas de contiguïté :
- Activer. L'interface est passive pour empêcher OSPF de former une contiguïté. OSPF annonce les réseaux reliés à des interfaces passives en tant que réseaux stub.
 - Désactiver : L'interface n'est pas passive et OSPF peut former une contiguïté. Il s'agit de l'option par défaut.
17. Dans le menu **type de réseau**, sélectionnez le type de réseau OSPF pour l'interface :
- Diffusion L'interface peut se connecter à plusieurs routeurs OSPF. Il s'agit de l'option par défaut.
 - **Point à point** : L'interface peut se connecter à un autre routeur OSPF.
18. Dans le menu **Authentication type**, sélectionnez si la communication sur l'interface est authentifiée et cryptée :
- Aucun : L'interface n'utilise ni l'authentification ni le cryptage. Il s'agit de l'option par défaut.
 - Tranquillité d'esprit L'interface vous invite à saisir une clé d'authentification. Cette clé est incluse (non cryptée) dans l'en-tête OSPF de tous les paquets envoyés sur le réseau. Tous les routeurs et commutateurs du réseau doivent être configurés avec la même clé.
 - Chiffrement L'interface vous invite à saisir une clé d'authentification et un ID d'authentification. Le chiffrement utilise l'algorithme MD5 message-Digest. Tous les routeurs et commutateurs du réseau doivent être configurés avec la même clé et le même ID.
19. Dans le champ **Authentication Key**, entrez la clé d'authentification OSPF de l'interface.
- Si vous sélectionnez **simple** dans le menu **type d'authentification**, vous pouvez définir une clé avec un maximum de 8 octets. Si vous sélectionnez **chiffrer** dans le menu **type d'authentification**, vous pouvez définir une clé de 16 octets maximum.
20. Dans le champ **Authentication Key ID**, entrez l'ID qui doit être utilisé pour l'authentification sur l'interface.
- Si vous sélectionnez **chiffrer** dans le menu **type d'authentification**, vous devez définir un ID, qui est un nombre compris entre 0 et 255.
21. Dans le champ **coût métrique**, entrez la valeur utilisée par OSPF pour calculer les chemins les plus courts.

La plage est de 1 à 65 535. Le numéro par défaut est 1.

22. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

23. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Champ	Description
Adresse IP	Adresse IP de l'interface.
Masque de sous-réseau	Masque de réseau, indiquant la partie de l'adresse IP qui identifie le réseau connecté
Intervalle d'accusé de réception LSA	Nombre de secondes que l'interface doit attendre avant d'envoyer un accusé de réception retardé
Etat	
État de l'interface OSPF :	
	inactif Il s'agit de l'état initial de l'interface. L'interface n'est pas utilisable pour OSPF et les paramètres d'interface sont à leurs valeurs initiales. Toutes les minuteries d'interface sont désactivées et aucune contiguïté n'est associée à l'interface.
	Bouclage : L'interface est rebouclée dans le matériel ou le logiciel. L'interface n'est pas disponible pour le trafic de données régulier. Vous pouvez obtenir des informations sur l'interface en envoyant des ping ICMP à l'interface ou via un test d'erreur de bit car les paquets IP peuvent toujours être adressés à une interface dans un état de bouclage. Une interface dans un état de bouclage est annoncée dans des LSA comme route hôte unique pour laquelle la destination est l'adresse de l'interface IP.
	PATIENTEZ ! Le commutateur surveille les paquets Hello reçus afin de détecter l'identité du routeur désigné de secours pour le réseau. Le commutateur ne peut pas sélectionner un routeur désigné de secours ou un routeur désigné tant que le processus n'est pas sorti de l'état d'attente. Cela évite les modifications inutiles du routeur désigné de sauvegarde.
	Routeur désigné : Le commutateur est le routeur désigné sur le réseau connecté. Des contiguïtés sont établies avec tous les autres routeurs et commutateurs du réseau. Le commutateur doit également émettre un LSA de réseau pour le nœud de réseau. Le réseau LSA contient des liens vers tous les commutateurs et routeurs (y compris le routeur désigné) du réseau.
	Routeur désigné de sauvegarde : Le commutateur est le routeur désigné de secours sur le réseau connecté. Le commutateur est promu au rang de routeur désigné si le routeur désigné actuel tombe en panne. Le commutateur établit des contiguïtés à tous les autres routeurs connectés au réseau. Le routeur désigné de sauvegarde exécute des fonctions légèrement différentes lors de l'inondation LSA, par rapport au routeur désigné.
	Autre routeur désigné : L'interface est connectée à une diffusion sur laquelle d'autres routeurs sont le routeur désigné et le routeur désigné de secours. Le commutateur tente de former des contiguïtés au routeur désigné et au routeur désigné de secours.
Routeur désigné	Identité du routeur désigné pour ce réseau, telle qu'elle est détectée par le routeur publicitaire. Le routeur désigné est identifié par son ID de routeur. La valeur 0.0.0.0 signifie qu'aucun routeur désigné n'est détecté.

(A continué)

Champ	Description
Routeur désigné de sauvegarde	Identité du routeur désigné de sauvegarde pour ce réseau, telle qu'elle est détectée par le routeur publicitaire. Le routeur désigné de sauvegarde est identifié par son ID de routeur. La valeur 0.0.0.0 signifie qu'aucun routeur désigné de sauvegarde n'est détecté.
Nombre d'événements Link	Nombre de fois que l'interface OSPF a changé d'état
LSA de liaison locale	Nombre de LSA opaques pour lesquels la portée d'inondation est le lien sur l'interface
Somme de contrôle LSA liaison locale	Somme des sommes de contrôle des LSA de liaison locale pour la liaison

Afficher ou effacer les statistiques OSPF d'une interface

Si OSPF est activé, vous pouvez afficher ou effacer les statistiques OSPF d'une interface.

Pour afficher ou effacer les statistiques OSPF d'une interface :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **routage > OSPF > Avancé > statistiques d'interface** .
La page statistiques de l'interface OSPF s'affiche.
6. Dans le menu **interface**, sélectionnez l'interface.
7. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).
8. Pour effacer tous les compteurs et réinitialiser toutes les statistiques de l'interface OSPF aux valeurs par défaut, cliquez sur le bouton **Effacer**.
9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Champ	Description
ID zone OSPF	Zone OSPF à laquelle appartient l'interface. Un ID de zone OSPF est un entier de 32 bits au format décimal à points qui identifie de manière unique la zone à laquelle l'interface se connecte.
Nombre de routeurs de bordure de zone	Le nombre de routeurs de bordure de zone (ABR) accessibles dans cette zone. Il est initialement nul et calculé à chaque passage SPF (Shortest Path First).
Nombre DE routeurs de bordure	Nombre total de routeurs périphériques de système autonome (AS) accessibles dans cette zone. Il est initialement nul, et est calculé à chaque passe SPF.
Décompte LSA zone	Nombre d'annonces d'état de lien dans la base de données d'état de lien de cette zone, à l'exclusion DES LSA externes.
Adresse IP	Adresse IP de l'interface.
Événements d'interface	Nombre de fois que l'interface OSPF a changé d'état ou qu'une erreur s'est produite.
Événements virtuels	Nombre de changements d'état ou d'erreurs survenus sur ce lien virtuel.
Événements voisins	Nombre de fois que cette relation de voisin a changé d'état ou qu'une erreur s'est produite.
Paquets envoyés :	Nombre de paquets OSPF transmis sur l'interface.
Paquets reçus :	Nombre de paquets OSPF valides reçus sur l'interface.
ABANDONNER	Nombre de paquets OSPF reçus rejetés en raison d'une erreur dans le paquet ou d'une erreur dans le traitement du paquet.
Version incorrecte	Nombre de paquets OSPF reçus pour lesquels le champ version de l'en-tête OSPF ne correspond pas à la version du processus OSPF traitant le paquet.
La source n'est pas sur le sous-réseau local	Nombre de paquets reçus rejetés car l'adresse IP source ne se trouve pas dans un sous-réseau configuré sur une interface locale.

(A continué)

Champ	Description
Lien virtuel introuvable	Nombre de paquets OSPF reçus rejetés parce que l'interface d'entrée se trouve dans une zone non dorsale et que l'en-tête OSPF a identifié le paquet comme appartenant au dorsal, mais qu'OSPF n'a pas de lien virtuel avec l'expéditeur du paquet.
Discordance de zone	Nombre de paquets OSPF rejetés car l'ID de zone dans l'en-tête OSPF n'est pas l'ID de zone configuré sur l'interface d'entrée.
Adresse IP de destination non valide.	Nombre de paquets OSPF rejetés car l'adresse IP de destination du paquet n'est pas l'adresse de l'interface d'entrée et n'est pas l'adresse multicast <i>AllDrouters</i> ou <i>AllSpfRouters</i> .
Type d'authentification incorrect	Nombre de paquets rejetés car le type d'authentification spécifié dans l'en-tête OSPF ne correspond pas au type d'authentification configuré sur l'interface d'entrée.
Echec de l'authentification	Nombre de paquets OSPF abandonnés en raison de l'échec de l'authentification avec le voisin. Cette authentification a lieu au niveau de l'interface.
Aucun voisin à l'adresse source	Nombre de paquets OSPF abandonnés parce que l'expéditeur n'est pas un voisin existant ou que l'adresse IP de l'expéditeur ne correspond pas à l'adresse IP enregistrée précédemment pour ce voisin.
Type de paquet OSPF non valide	Nombre de paquets OSPF rejetés car le champ type de paquet dans l'en-tête OSPF n'est pas un type connu.
Hellos ignoré	Nombre de paquets Hello reçus ignorés par l'interface. Ce sont les paquets Hello des nouveaux voisins après que la limite a été atteinte pour le nombre de voisins sur l'interface ou sur le commutateur.
Hellos envoyés	Nombre de paquets Hello envoyés sur l'interface.
Hellos reçus	Nombre de paquets Hello reçus sur l'interface.
Paquets DD envoyés	Nombre de paquets DD (Database description) envoyés sur l'interface.
Paquets DD reçus	Nombre de paquets de description de base de données reçus sur l'interface.
Demandes LS envoyées	Nombre de requêtes d'état de liaison (LS) envoyées sur l'interface.
Demandes LS reçues	Nombre de demandes d'état de liaison reçues sur l'interface.
Mises à jour LS envoyées	Nombre de mises à jour de l'état de la liaison envoyées sur l'interface.
Mises à jour LS reçues	Nombre de mises à jour de l'état de la liaison reçues sur l'interface.
Accusés de réception LS envoyés	Nombre d'accusés de réception d'état de liaison envoyés sur l'interface.
Accusés de réception LS reçus	Nombre d'accusés de réception d'état de liaison reçus sur l'interface.

Afficher ou effacer les informations de voisinage OSPF pour une interface

Si OSPF est activé, vous pouvez afficher les voisins OSPF. Vous pouvez également effacer les informations de voisinage OSPF.

Pour afficher ou effacer les informations de voisinage OSPF d'une interface :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > OSPF > Avancé > table de voisinage** .

La page table de voisinage OSPF s'affiche.

6. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

7. Pour effacer les informations de voisinage OSPF, en rétablissant les valeurs par défaut des champs de la table, cliquez sur le bouton **Effacer**.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Champ	Description
Interface	Interface pour laquelle les données sont affichées.
Adresse IP du voisin	Adresse IP de l'interface du routeur voisin connectée au réseau. L'adresse IP du voisin est apprise lorsque des paquets Hello sont reçus du voisin. Pour les liaisons virtuelles, l'adresse IP du voisin est apprise lors du processus de construction de la table de routage. L'adresse IP du voisin est utilisée dans les situations suivantes : • Comme adresse IP de destination lorsque les paquets de protocole sont envoyés en tant que paquets unicast le long de cette contiguïté. • Dans un routeur LSA comme ID de liaison pour le réseau connecté si le routeur voisin est sélectionné comme routeur désigné.
Index de l'interface voisine	Combinaison unité/logement/port qui identifie l'index de l'interface voisine.
Code ID du routeur	Entier de 32 bits au format décimal à points qui représente l'interface voisine.
ID zone	ID de zone de la zone OSPF associée à l'interface.
Options	Valeur entière qui indique les fonctionnalités OSPF facultatives prises en charge par le voisin. Les capacités optionnelles OSPF du voisin sont également répertoriées dans ses paquets Hello. Les informations Options permettent de rejeter les paquets Hello reçus en cas de non-concordance dans certaines capacités OSPF. (Si les paquets Hello sont rejetés, par exemple, les relations de voisinage ne peuvent pas être formées.)
Priorité du routeur	Priorité OSPF pour l'interface. La priorité d'une interface est un entier de priorité compris entre 0 et 255. La valeur 0 indique que le routeur n'est pas éligible pour devenir le routeur désigné sur ce réseau.
Etat	L'état du voisin OSPD : inactif Il s'agit de l'état initial d'une conversation de voisinage. Il indique qu'aucune information récente n'a été reçue du voisin. Sur les réseaux à accès multiple non diffusé (NBMA), les paquets Hello peuvent toujours être envoyés aux voisins à l'état inactif, bien qu'à une fréquence réduite. Tentative: Cet état n'est valide que pour les voisins connectés à des réseaux NBMA. Il indique qu'aucune information récente n'a été reçue du voisin, mais qu'un effort plus concerté doit être fait pour contacter le voisin. Cela se fait en envoyant les paquets Hello voisins à intervalles Hello. Init Un paquet Hello a récemment été détecté en provenance du voisin. Cependant, la communication bidirectionnelle n'est pas encore établie avec le voisin (par exemple, le routeur n'est pas inclus dans le paquet Hello du voisin). Tous les voisins dans cet état ou dans un état listé ci-dessous dans ce tableau sont inclus dans les paquets Hello envoyés depuis l'interface associée. 2 voies: La communication entre les deux interfaces de routage est bidirectionnelle. Ceci est assuré par le fonctionnement du protocole Hello. Il s'agit de l'état le plus avancé à moins de commencer l'établissement de la contiguïté. Le routeur désigné de sauvegarde est sélectionné parmi l'ensemble de voisins dans l'état bidirectionnel ou un état répertorié ci-dessous dans ce tableau. Début d'échange : Il s'agit de la première étape de la création d'une contiguïté entre les deux interfaces de routage voisines. Le processus dans cet état détermine quel routeur est le maître et quel est le numéro de séquence DD initial. Les conversations voisines dans cet état ou dans un état répertorié ci-dessous dans ce tableau sont appelées contiguïtés.

(A continué)

Champ	Description
Échange: Les interfaces de routage incluent toute sa base de données d'état de liens dans des paquets de description de base de données qu'elle envoie au voisin. Le routeur peut également envoyer des paquets de demande d'état de liaison pour demander les LSA les plus récents du voisin. Toutes les contiguïtés dans l'état Exchange ou dans un état répertorié ci-dessous dans ce tableau sont utilisées par la procédure d'inondation. Ces contiguïtés peuvent transmettre et recevoir tous les types de paquets de protocole de routage OSPF.	
Chargement Les paquets de demande d'état de liaison sont envoyés au voisin demandant les LSA les plus récents qui ont été découverts mais pas encore reçus dans l'état Exchange.	
Complet: Les routeurs voisins sont entièrement adjacents. Ces contiguïtés sont désormais incluses dans les LSA de routeur et les LSA de réseau.	
Événements	Nombre de fois que cette relation de voisin a changé d'état ou qu'une erreur s'est produite.
Permanence	Statut de l'entrée. Dynamique et permanente font référence à la façon dont le voisin est devenu connu.
Hellos supprimés	Cela indique si les hellos sont supprimés pour le voisin.
Longueur de la file d'attente de retransmission	Entier représentant la longueur actuelle de la file d'attente de retransmission de l'ID de routeur voisin spécifié de l'interface spécifiée.
Durée de fonctionnement	Temps de disponibilité voisin, qui indique le temps écoulé depuis que la contiguïté a atteint l'état complet pour la dernière fois.
Temps mort	Durée en secondes pendant laquelle le commutateur attend avant de déterminer que le voisin est inaccessible.

Affichez la base de données d'état des liens OSPF

Si OSPF est activé, vous pouvez afficher la base de données d'état des liens OSPF.

Pour afficher la base de données d'état des liens OSPF :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > OSPF > Avancé > base de données d'état des liens** .

La page affiche les sections base de données d'état des liens, table LSDB externe et table LSDB opaque.

Le terme LSDB signifie Link State Database ; le terme AS signifie système autonome.

6. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

Les tableaux suivants décrivent les champs en lecture seule de la page.

Table 123 : Lier la base de données d'état

Champ	Description
Code ID du routeur	Nombre de 32 bits au format décimal à points qui identifie le commutateur dans le système autonome (AS). Pour modifier l'ID du routeur, vous devez d'abord désactiver OSPF. Après avoir défini un nouvel ID de routeur, vous devez réactiver OSPF pour que la modification prenne effet. La valeur par défaut est 0,0,0,0, bien qu'il ne s'agisse pas d'un ID de routeur valide.
ID zone	ID de la zone OSPF à laquelle l'une des interfaces de commutateur est connectée. Un ID de zone est un entier de 32 bits au format décimal à points qui identifie de manière unique la zone à laquelle une interface est connectée.
Type de LSA	Le format et la fonction de l'annonce d'état de lien: Illégal ; liens de routeur ; liens réseau ; Résumé réseau ; Résumé ASBR ; AS-externe ; membre de groupe ; NSSA ; TMP2 ; lien opaque ; zone opaque ; AS opaque ; inconnu.
ID LS	L'ID d'état de liaison identifie la partie du domaine de routage décrite par l'annonce. La valeur de l'ID LS dépend du type LS de la publicité.
Age :	Temps en secondes écoulé depuis que l'annonce d'état de lien a été émise pour la première fois.

Table 123 : Lier la base de données d'état (A continué)

Champ	Description
Séquence	Entier de 32 bits signé utilisé pour détecter les annonces d'état de lien anciennes et dupliquées. Plus le numéro de séquence est grand, plus la publicité est récente.
Total de contrôle	Somme de contrôle du contenu complet de la publicité, à l'exception du champ LS Age. La somme de contrôle est utilisée pour détecter la corruption de données d'une publicité. Cette corruption peut se produire lorsqu'une publicité est inondée ou lorsqu'elle est conservée dans la mémoire d'un routeur.
Options	Le champ Options de l'en-tête annonce état de lien indique les fonctionnalités facultatives associées à l'annonce : • Q: Active la prise en charge de l'ingénierie du trafic QoS. • E Spécifie la manière DONT les LSA externes sont inondés. • MC Spécifie la manière dont les datagrammes de multidiffusion IP sont transmis conformément aux spécifications standard. • O: Spécifie si les LSA opaques sont pris en charge. • v Spécifie si les extensions OSPF pour classe de service (cos) et VPN sont prises en charge.

Table 124 : Table LSDB externe

Champ	Description
Code ID du routeur	Nombre de 32 bits au format décimal à points qui identifie le commutateur dans le système autonome (AS). Pour modifier l'ID du routeur, vous devez d'abord désactiver OSPF. Après avoir défini un nouvel ID de routeur, vous devez réactiver OSPF pour que la modification prenne effet. La valeur par défaut est 0,0,0,0, bien qu'il ne s'agisse pas d'un ID de routeur valide.
Type de LSA	Le format et la fonction de l'annonce d'état de lien: Résumé ASBR ; AS-externe ; NSSA ; ou TMP2.
ID LS	L'ID d'état de liaison identifie la partie du domaine de routage décrite par l'annonce. La valeur de l'ID LS dépend du type LS de la publicité.
Age :	Temps en secondes écoulé depuis que l'annonce d'état de lien a été émise pour la première fois.
Séquence	Entier de 32 bits signé utilisé pour détecter les annonces d'état de lien anciennes et dupliquées. Plus le numéro de séquence est grand, plus la publicité est récente.
Total de contrôle	Somme de contrôle du contenu complet de la publicité, à l'exception du champ LS Age. La somme de contrôle est utilisée pour détecter la corruption de données d'une publicité. Cette corruption peut se produire lorsqu'une publicité est inondée ou lorsqu'elle est conservée dans la mémoire d'un routeur.

Table 125 : COMME table LSDB opaque

Champ	Description
Code ID du routeur	Nombre de 32 bits au format décimal à points qui identifie le commutateur dans le système autonome (AS). Pour modifier l'ID du routeur, vous devez d'abord désactiver OSPF. Après avoir défini un nouvel ID de routeur, vous devez réactiver OSPF pour que la modification prenne effet. La valeur par défaut est 0,0,0,0, bien qu'il ne s'agisse pas d'un ID de routeur valide.
Type de LSA	Le format et la fonction de l'annonce d'état de lien: Zone opaque ; COMME opaque ; ou lien opaque.
ID LS	L'ID d'état de liaison identifie la partie du domaine de routage décrite par l'annonce. La valeur de l'ID LS dépend du type LS de la publicité.
Age :	Temps en secondes écoulé depuis que l'annonce d'état de lien a été émise pour la première fois.
Séquence	Entier de 32 bits signé utilisé pour détecter les annonces d'état de lien anciennes et dupliquées. Plus le numéro de séquence est grand, plus la publicité est récente.
Total de contrôle	Somme de contrôle du contenu complet de la publicité, à l'exception du champ LS Age. La somme de contrôle est utilisée pour détecter la corruption de données d'une publicité. Cette corruption peut se produire lorsqu'une publicité est inondée ou lorsqu'elle est conservée dans la mémoire d'un routeur.

Configurer un lien virtuel OSPF

Si vous ne pouvez pas configurer une liaison physique entre le commutateur et la zone de backbone OSPF, vous pouvez ajouter une liaison virtuelle pour vous connecter à la zone de backbone via une zone commune (non backbone). Vous pouvez configurer une liaison virtuelle entre tous les routeurs de bordure de zone qui ont des interfaces physiques avec la zone commune.

Pour configurer un lien virtuel OSPF :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > OSPF > Avancé > Configuration de liaison virtuelle**.

La page Configuration du lien virtuel OSPF s'affiche.

6. Dans le champ **ID de zone**, saisissez un ID de zone OSPF.

Un ID de zone est un entier de 32 bits au format décimal à points qui identifie de manière unique la zone à laquelle une interface est connectée.

7. Dans le champ **ID du routeur voisin**, entrez la partie voisine d'une spécification de lien virtuel.

8. Dans le champ **Hello Interval**, entrez l'intervalle Hello OSPF de l'interface.

Cet intervalle doit être le même pour tous les routeurs et commutateurs du réseau. L'intervalle est compris entre 1 et 65 535 secondes. La valeur par défaut est 10 secondes.

9. Dans le champ **intervalle mort**, entrez le nombre de secondes pendant lesquelles l'interface attend les paquets Hello d'un voisin avant de déterminer que ce voisin est en panne.

Cet intervalle doit être le même pour tous les routeurs et commutateurs du réseau. Cet intervalle doit être un multiple de l'intervalle Hello. L'intervalle est compris entre 1 et 65 535. La valeur par défaut est de 40 secondes. (L'intervalle Hello par défaut est de 10 secondes.)

10. Dans le champ **Iftransit Delay Interval**, entrez le nombre estimé de secondes nécessaires pour transmettre un paquet de mise à jour de l'état de la liaison sur l'interface.

L'intervalle est compris entre 1 et 3600 secondes (1 heure). La valeur par défaut est 1 seconde.

11. Dans le champ **intervalle de retransmission**, entrez le nombre de secondes entre les annonces d'état de liaison pour les contiguïtés, c'est-à-dire pour les périphériques voisins qui forment une contiguïté OSPF avec l'interface.

L'intervalle est également utilisé lors de la retransmission de descriptions de base de données et de paquets de demande d'état de liens. La valeur de l'intervalle est comprise entre 1 et 3600 secondes (1 heure). La valeur par défaut est de 5 secondes.

12. Dans le menu **Authentication type**, sélectionnez si la communication sur l'interface est authentifiée et cryptée :

- **Aucun** : L'interface n'utilise ni l'authentification ni le cryptage. Il s'agit de l'option par défaut.
- **Tranquillité d'esprit** L'interface vous invite à saisir une clé d'authentification. Cette clé est incluse (non cryptée) dans l'en-tête OSPF de tous les paquets envoyés sur le réseau. Tous les routeurs et commutateurs du réseau doivent être configurés avec la même clé.
- **Chiffrement** L'interface vous invite à saisir une clé d'authentification et un ID d'authentification. Le chiffrement utilise l'algorithme MD5 message-Digest. Tous les routeurs et commutateurs du réseau doivent être configurés avec la même clé et le même ID.

13. Dans le champ **Authentication Key**, entrez la clé d'authentification OSPF de l'interface.

Si vous sélectionnez **simple** dans le menu **type d'authentification**, vous pouvez définir une clé avec un maximum de 8 octets. Si vous sélectionnez **chiffrer** dans le menu **type d'authentification**, vous pouvez définir une clé de 16 octets maximum.

14. Dans le champ **Authentication ID**, entrez l'ID qui doit être utilisé pour l'authentification sur l'interface.

Si vous sélectionnez **chiffrer** dans le menu **type d'authentification**, vous devez définir un ID, qui est un nombre compris entre 0 et 255.

15. Cliquez sur le bouton **Add** (Ajouter).

Les paramètres sont enregistrés.

16. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Champ	Description
Etat voisin	
État de l'interface voisine OSPF :	
inactif Il s'agit de l'état initial de l'interface. L'interface n'est pas utilisable pour OSPF et les paramètres d'interface sont à leurs valeurs initiales. Toutes les minuteries d'interface sont désactivées et aucune contiguïté n'est associée à l'interface.	

(A continué)

Champ	Description
	Bouclage : L'interface est rebouclée dans le matériel ou le logiciel. L'interface n'est pas disponible pour le trafic de données régulier. Vous pouvez obtenir des informations sur l'interface en envoyant des ping ICMP à l'interface ou via un test d'erreur de bit car les paquets IP peuvent toujours être adressés à une interface dans un état de bouclage. Une interface dans un état de bouclage est annoncée dans des LSA comme route hôte unique pour laquelle la destination est l'adresse de l'interface IP.
	PATIENTEZ ! Le dispositif voisin surveille les paquets Hello reçus afin de détecter l'identité du routeur désigné de secours pour le réseau. Le périphérique voisin ne peut pas sélectionner un routeur désigné de secours ou un routeur désigné tant que informatique n'est pas sorti de l'état d'attente. Cela évite les modifications inutiles du routeur désigné de sauvegarde.
	Routeur désigné : Le périphérique voisin est le routeur désigné sur le réseau connecté. Des contiguïtés sont établies avec tous les autres routeurs et commutateurs du réseau. Le périphérique voisin doit également émettre un LSA de réseau pour le nœud de réseau. Le réseau LSA contient des liens vers tous les commutateurs et routeurs (y compris le routeur désigné) du réseau.
	Routeur désigné de sauvegarde : Le périphérique voisin est le routeur désigné de sauvegarde sur le réseau connecté. Le périphérique voisin est promu au rang de routeur désigné si le routeur désigné actuel tombe en panne. Le dispositif voisin établit des contiguïtés à tous les autres routeurs reliés au réseau. Le routeur désigné de sauvegarde exécute des fonctions légèrement différentes lors de l'inondation LSA, par rapport au routeur désigné.
	Autre routeur désigné : L'interface est connectée à une diffusion sur laquelle d'autres routeurs sont le routeur désigné et le routeur désigné de secours. Le périphérique voisin tente de former des contiguïtés à la fois avec le routeur désigné et le routeur désigné de secours.
Etat	L'état de l'interface du commutateur OSPF :
	inactif Il s'agit de l'état initial de l'interface. L'interface n'est pas utilisable pour OSPF et les paramètres d'interface sont à leurs valeurs initiales. Toutes les minuteries d'interface sont désactivées et aucune contiguïté n'est associée à l'interface.
	Bouclage : L'interface est rebouclée dans le matériel ou le logiciel. L'interface n'est pas disponible pour le trafic de données régulier. Vous pouvez obtenir des informations sur l'interface en envoyant des ping ICMP à l'interface ou via un test d'erreur de bit car les paquets IP peuvent toujours être adressés à une interface dans un état de bouclage. Une interface dans un état de bouclage est annoncée dans des LSA comme route hôte unique pour laquelle la destination est l'adresse de l'interface IP.
	PATIENTEZ ! Le commutateur surveille les paquets Hello reçus afin de détecter l'identité du routeur désigné de secours pour le réseau. Le commutateur ne peut pas sélectionner un routeur désigné de secours ou un routeur désigné tant que le informatique n'est pas sorti de l'état d'attente. Cela évite les modifications inutiles du routeur désigné de sauvegarde.
	Routeur désigné : Le commutateur est le routeur désigné sur le réseau connecté. Des contiguïtés sont établies avec tous les autres routeurs et commutateurs du réseau. Le commutateur doit également émettre un LSA de réseau pour le nœud de réseau. Le réseau LSA contient des liens vers tous les commutateurs et routeurs (y compris le routeur désigné) du réseau.
	Routeur désigné de sauvegarde : Le commutateur est le routeur désigné de secours sur le réseau connecté. Le commutateur est promu au rang de routeur désigné si le routeur désigné actuel tombe en panne. Le commutateur établit des contiguïtés à tous les autres routeurs connectés au réseau. Le routeur désigné de sauvegarde exécute des fonctions légèrement différentes lors de l'inondation LSA, par rapport au routeur désigné.

(A continué)

Champ	Description
Autre routeur désigné	L'interface est connectée à une diffusion sur laquelle d'autres routeurs sont le routeur désigné et le routeur désigné de secours. Le commutateur tente de former des contiguïtés au routeur désigné et au routeur désigné de secours.
Métrique	Valeur métrique utilisée par le lien virtuel pour calculer les chemins les plus courts.

Configurez la redistribution de route OSPF

La redistribution de route (RR) permet au commutateur de partager des informations de routage entre des routeurs connectés localement (ou des interfaces de routage) et entre différents protocoles de routage, tels que OSPF et RIP, ainsi que des informations sur les routes statiques.

Pour configurer la redistribution de route OSPF :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **rou tage > OSPF > Avancé > redistribution de route** .

La page redistribution de route OSPF s'affiche.

6. En regard du champ **source**, cochez la case correspondant à un ou plusieurs types de routes sources auxquels la configuration s'applique :

- Connecté Routes entre les routeurs connectés localement (ou interfaces de routage).
- Statique Routes configurées manuellement.
- RIP Routes détectées par le protocole RIP (Routing information Protocol).

7. Dans le menu **redistribuer**, sélectionnez si la redistribution est activée :

- Activer. Le type de route peut être redistribué.
- Désactiver : Le type de route ne peut pas être redistribué.

8. Dans le champ **valeur métrique**, définissez la valeur métrique du type de route.

Si le type de route est préconfiguré, la valeur métrique s'affiche, mais vous pouvez modifier informatique. La plage est de 0 à 16777214.

9. Dans le menu **type de métrique**, sélectionnez le type de métrique à utiliser pour le type de route :

- **Externe type 1** : Métriques externes de type 1 comparables à la métrique OSPF.
- **Externe type 2** : Métriques externes de type 2 supposées supérieures au coût de la métrique OSPF.

10. Dans le champ **balise**, définissez la balise du type de route.

Si le type de route est préconfiguré, la balise s'affiche, mais vous pouvez modifier informatique. La plage est de 0 à 4294967295.

11. Dans le menu **Subnets**, indiquez si les routes en sous-réseaux peuvent être redistribuées :

- Activer. Les routes en sous-réseaux peuvent être redistribuées.
- Désactiver : Les routes en sous-réseaux ne peuvent pas être redistribuées.

12. Dans le champ **liste de distribution**, spécifiez une liste de contrôle d'accès (ACL) existante qui filtre les routes à redistribuer par le protocole de destination.

Seules les routes autorisées sont redistribuées. Si vous entrez une ACL inexistante, toutes les routes sont autorisées. La plage des ID ACL est comprise entre 1 et 199.

Pour le filtrage des routes, seuls les champs ACL suivants sont utilisés :

- **Adresse IP source et masque de réseau** : L'adresse IP source est comparée à l'adresse IP de destination de la route. Le masque de réseau IP source est traité comme un masque générique, indiquant quels bits de l'adresse IP source doivent

correspondre à l'adresse de destination de la route. (Un 1 dans le masque indique un message « *ne pas prendre en compte* » dans le bit d'adresse correspondant.)

- **Adresse IP de destination et masque de réseau** : L'adresse IP de destination est comparée à l'adresse IP source de la route. Le masque de réseau IP de destination est traité comme un masque générique, indiquant quels bits de l'adresse IP de destination doivent correspondre à l'adresse source de la route. (Un 1 dans le masque indique un message « *ne pas prendre en compte* » dans le bit d'adresse correspondant.)
- Action : Autoriser ou refuser.

Tous les autres champs de la liste de contrôle d'accès (port source et de destination, priorité, ToS, etc.) sont ignorés.

13. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

14. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurer le transfert sans arrêt OSPF

Le transfert non-stop (NSF) OSPF garantit que le routage OSPF se poursuit en laissant temporairement d'autres périphériques du réseau effectuer le routage OSPF pour le commutateur. Cela signifie que même si le commutateur redémarre, le routage OSPF peut continuer. (Nous appelons ce type de processus de redémarrage un redémarrage normal.) Vous pouvez configurer si OSPF NSF est activé sur le commutateur et si le commutateur peut prendre en charge les événements OSPF NSF sur les voisins, c'est-à-dire aider les voisins à redémarrer correctement.

Pour configurer OSPF NSF :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > OSPF > Avancé > Résumé OSPF NSF**.

La page Récapitulatif NSF OSPF s'affiche.

6. Dans le menu **mode support**, sélectionnez la manière dont le commutateur effectue un redémarrage normal :

- **Toujours**: OSPF effectue un redémarrage progressif pour tous les événements de redémarrage à chaud planifiés et non planifiés.
- Désactivé : Les redémarrages progressifs OSPF sont désactivés. Il s'agit de la sélection par défaut.
- **Planifié** : OSPF n'effectue un redémarrage normal que si un redémarrage est planifié (par exemple, parce qu'une commande CLI est exécutée).

7. Dans le champ **intervalle de redémarrage**, entrez le temps que le commutateur attend après un redémarrage progressif avant de poursuivre le routage OSPF.

La plage est de 0 à 1800 secondes. La valeur par défaut est de 120 secondes.

8. Dans le menu **Helper support mode**, indiquez si le commutateur peut prendre en charge un voisin qui effectue un redémarrage à chaud :

- **Toujours**: OSPF aide un voisin à redémarrer pour tous les événements de redémarrage à chaud planifiés et non planifiés. Il s'agit de la sélection par défaut.
- Désactivé : OSPF n'aide pas un voisin à redémarrer.
- **Planifié** : OSPF aide un voisin à redémarrer uniquement si le redémarrage est planifié.

9. Dans le menu **Helper strict LSA Checking**, sélectionnez si le commutateur quitte le mode support Helper lorsque la topologie change :

- Activer. Le commutateur quitte le mode de support d'assistance lorsque la topologie change. Il s'agit de la sélection par défaut.
- Désactiver : Le commutateur ne quitte pas le mode de prise en charge de l'assistant lorsque la topologie change.

10. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

11. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Champ	Description
Etat de redémarrage	État de redémarrage du mode de prise en charge de l'assistant OSPF : • Ne redémarre pas • Redémarrage planifié • Redémarrage non planifié
Âge de redémarrage (s)	Temps en secondes écoulé depuis le dernier redémarrage.
Motif de sortie du redémarrage	Affiche le dernier démarrage du processus de routage OSPF sur le commutateur : • Non tenté : Aucune tentative de redémarrage normal n'a été effectuée. • Progression Un redémarrage normal est en cours. • Terminé Le redémarrage normal précédent s'est terminé avec succès. • Délai expiré : Le délai du redémarrage normal précédent a expiré. • Topologie modifiée : Le redémarrage progressif précédent s'est terminé prématurément en raison d'une modification de topologie.

Open Shortest Path First version 3

Open Shortest Path First version 3 (OSPFv3) est le protocole de routage OSPF pour IPv6. Informatique est similaire à OSPFv2 (généralement simplement appelé OSPF) dans son concept de base de données d'état de liens, intra- et inter-zone, et EN TANT QUE routes externes et liens virtuels.

Vous pouvez utiliser OSPF et OSPFv3 simultanément : OSPF fonctionne avec IPv4 et OSPFv3 avec IPv6.

OSPFv3 diffère de OSPF à plusieurs égards :

- L'appairage se fait par le biais d'adresses lien-local
- Le protocole est basé sur la liaison plutôt que sur le réseau

- Les changements d'adresse sont communiqués via les annonces d'état de lien (LSA) LEAF, qui permettent finalement son utilisation pour IPv4 et IPv6
- Les liaisons point à point sont prises en charge pour permettre le fonctionnement sur des tunnels

Activer le OSPFv3

Avant qu'OSPFv3 ne devienne opérationnel, vous devez activer le mode d'administration pour le routage IPv6 sur le commutateur (voir [Gérer les paramètres de routage IPv6 globaux](#) à la page 545).

Pour activer OSPFv3 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > OSPFv3 > Basic > OSPFv3 Configuration**.

La page Configuration OSPFv3 s'affiche.

6. Sélectionnez un bouton radio mode Admin :

- Activer. OSPFv3 est activé pour le commutateur. Il s'agit de l'option par défaut.
- Désactiver : OSPFv3 est désactivé pour le commutateur.

Le champ ID routeur affiche le nombre 32 bits au format décimal à points. Ce numéro identifie de manière unique le commutateur au sein du système autonome (AS).

Pour modifier l'ID du routeur, vous devez d'abord désactiver OSPFv3. Après avoir défini un nouvel ID de routeur, vous devez réactiver OSPFv3 pour que la modification prenne effet. La valeur par défaut est 0,0.0,0, bien qu'il ne s'agisse pas d'un ID de routeur valide.

7. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez l'annonce de route par défaut OSPFv3

Qu'une route par défaut existe ou non dans la table de routage, vous pouvez configurer une route par défaut pour les annonces OSPFv3, y compris une valeur de métrique et un type de métrique.

Pour configurer l'annonce de route par défaut OSPFv3 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > OSPFv3 > Avancé > Configuration OSPFv3**.

La page Configuration OSPFv3 s'affiche. La page affiche différentes sections.

6. Accédez à la section Configuration d'annonce de route par défaut.

7. Sélectionnez un bouton radio d'origine des informations par défaut :

- Activer. OSPFv3 génère une route par défaut pour les annonces d'état de liens externes (LSA). Cette route est au format adresse/préfixe IPv6.
- Désactiver : OSPFv3 ne génère pas de route par défaut pour les LSA externes. Il s'agit de l'option par défaut.

8. Sélectionnez un bouton radio toujours :

- Vrai OSPFv3 génère une route par défaut, qu'une route par défaut existe ou non.
- Faux OSPFv3 génère une route par défaut uniquement si une route par défaut se trouve déjà dans la table de routage du commutateur.

9. Dans le champ **métrique**, définissez la valeur métrique de l'itinéraire par défaut.

La valeur est comprise entre 0 et 16777214. Le numéro par défaut est 0.

10. Bouton radio sélectionner un champ type d'audit :

- **Externe type 1** : Cette métrique est calculée en ajoutant le coût interne OSPFv3 au coût externe redistribué.
- **Externe type 2** : Cette métrique est calculée en utilisant uniquement le coût redistribué externe. Il s'agit de la valeur par défaut.

11. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

12. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez les paramètres OSPFv3 globaux

.

Vous pouvez configurer les paramètres OSPFv3 qui s'appliquent globalement aux processus OSPFv3 sur le commutateur.

Pour configurer les paramètres OSPFv3 globaux :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > OSPFv3 > Avancé > Configuration OSPFv3**.

La page Configuration OSPFv3 s'affiche. La page affiche différentes sections.

6. Accédez à la section Configuration OSPFv3.

7. Dans le champ **Router ID (ID du routeur)**, entrez le nombre de 32 bits au format décimal à points qui identifie de manière unique le routeur au sein du système autonome (AS).

Pour modifier l'ID du routeur, vous devez d'abord désactiver OSPFv3. Après avoir défini un nouvel ID de routeur, vous devez réactiver OSPFv3 pour que la modification

prenne effet. La valeur par défaut est 0,0.0,0, bien qu'il ne s'agisse pas d'un ID de routeur valide.

8. Sélectionnez un bouton radio mode Admin :
 - Activer. OSPFv3 est activé pour le commutateur. Il s'agit de l'option par défaut.
 - Désactiver : OSPFv3 est désactivé pour le commutateur.

Avant qu'OSPFv3 ne devienne opérationnel, vous devez activer le mode d'administration pour le routage IPv6 sur le commutateur (voir [Configurer les interfaces de routage IPv6](#) à la page 548).

9. Dans le champ **intervalle de débordement de sortie**, définissez le nombre de secondes que OSPFv3 doit attendre avant de quitter un état de débordement.

Lorsque le nombre de LSA externes autres que ceux par défaut dépasse une limite, le commutateur entre dans un état de dépassement dans lequel OSPFv3 ne peut pas émettre de LSA externes autres que ceux par défaut. (Pour plus d'informations, voir RFC 1765.)

Si le nombre de secondes est 0 (paramètre par défaut), OSPFv3 ne quitte pas l'état de dépassement jusqu'à ce que vous désactiviez et réactiviez OSPFv3. La valeur maximale peut être de 2 147 483 647 secondes.

10. Dans le champ **External LSDB Limit**, définissez la limite de la base de données d'état de liens externe (LSDB) pour OSPFv3.

La base de données d'état des liens du routeur ne peut pas contenir plus de LSA AS-External-LSA que la limite définie pour la carte LSDB externe.

La limite de la carte LSDB externe doit être définie de manière identique sur tous les routeurs rattachés au backbone OSPFv3 ou à toute zone OSPFv3 normale. La limite peut être comprise entre -1 et 2147483647. Le paramètre par défaut est -1, ce qui indique qu'il n'y a pas de limite.

11. Dans le champ **mesure par défaut**, définissez la mesure par défaut des routes redistribuées.

La plage est de 1 à 16777214. Le numéro par défaut est 0.

12. Dans le champ **chemins maximum**, définissez le nombre de chemins que OSPFv3 peut signaler pour une destination.

La plage est de 1 à 16. Le numéro par défaut est 16.

13. Dans le champ **bande passante de référence autocoût**, définissez la bande passante qui contrôle la façon dont OSPFv3 calcule le coût de la liaison.

Définissez la bande passante de référence en mégabits par seconde. À moins qu'un coût de liaison ne soit configuré, le coût de liaison est calculé en divisant la largeur de bande de référence par la largeur de bande de l'interface. La plage est de 1 à 4294967. Le numéro par défaut est 100.

14. Dans le menu **Default passive Setting**, configurez le paramètre global du mode passif pour toutes les interfaces OSPFv3 :
 - Activer. Le réglage du mode passif global est activé. OSPFv3 ne forme pas de contiguïtés sur les interfaces passives, mais annonce les réseaux attachés comme des réseaux stub.
 - Désactiver : Le réglage du mode passif global est désactivé. La valeur par défaut est désactiver.
 15. Dans le menu **Helper support mode**, indiquez si le commutateur peut prendre en charge un voisin qui effectue un redémarrage à chaud dans une configuration de transfert sans arrêt (NSF) OSPFv3 :
 - **Toujours**: OSPFv3 aide un voisin de redémarrage pour tous les événements de redémarrage à chaud planifiés et non planifiés. Il s'agit de la sélection par défaut.
 - Désactivé : OSPFv3 n'aide pas un voisin redémarrant.
 - **Planifié** : OSPFv3 aide un voisin à redémarrer uniquement si le redémarrage est planifié.
 16. Dans le menu **Helper strict LSA Checking**, sélectionnez si le commutateur quitte le mode de support Helper (pour OSPFv3 NSF) lorsque la topologie change :
 - Activer. Le commutateur quitte le mode de support d'assistance lorsque la topologie change. Il s'agit de la sélection par défaut.
 - Désactiver : Le commutateur ne quitte pas le mode de prise en charge de l'assistant lorsque la topologie change.
 17. Cliquez sur le bouton **Apply** (Appliquer).
- Les paramètres sont enregistrés.
18. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Champ	Description
Mode ASBR	Indique si l'interface de routage fonctionne comme un routeur de limite de système autonome (ASBR). Un ASBR peut être configuré pour redistribuer des routes à partir d'un autre protocole ou pour émettre des LSA externes qui annoncent la route par défaut.
Etat ABR	Indique si l'interface de routage fonctionne comme un routeur de bordure de zone (ABR). Un ABR possède des interfaces non virtuelles actives dans deux ou plusieurs zones OSPFv3.
Décompte LSA externe	Nombre d'annonces d'état de lien (LSA) externes (LS type 5) dans la base de données d'état de lien.

(A continué)

Champ	Description
Somme de contrôle LSA externe	Somme des sommes de contrôle LS des LSA externes contenues dans la base de données d'état des liens. Vous pouvez utiliser cette somme pour déterminer s'il y a eu un changement dans la base de données d'état des liaisons d'un commutateur ou d'un routeur, et pour comparer les bases de données d'état des liaisons de deux unités. Cette valeur est en hexadécimal.
De nouveaux LSA ont été créés	Nombre de LSA émis par le commutateur. Dans toute zone OSPFv3, un routeur (ou dans ce cas, un commutateur) émet plusieurs LSA. Chaque routeur émet un routeur-LSA. Si le routeur est également le routeur désigné pour l'un des réseaux de la zone, informatique émet des LSA réseau pour ces réseaux.
LSA reçus	Nombre de LSA reçus pour les nouvelles instanciations. Ce nombre n'inclut pas les nouvelles instanciations de LSA auto-initiées.

Ajouter ou supprimer un ID de zone commune OSPFv3

Une zone commune OSPFv3 se compose d'un groupe de périphériques partageant le même ID de zone.

Pour ajouter ou supprimer un ID de zone commune OSPFv3 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > OSPFv3 > Avancé > Configuration de la zone commune**.

La page Configuration de la zone commune OSPFv3 s'affiche.

6. Dans le champ **ID de zone**, entrez un ID de zone OSPFv3.

Un ID de zone est un entier de 32 bits au format décimal à points qui identifie de manière unique la zone à laquelle une interface est connectée.

7. Effectuez l'une des actions suivantes :

- Ajouter Cliquez sur le bouton **Add** (Ajouter).
ID de zone ajouté.
- Supprimer Cliquez sur le bouton **Supprimer**.
ID de zone supprimé.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Champ	Description
Routage externe	Une définition des capacités du commutateur pour la zone, y compris si oui ou non des AS-externes-LSA sont inondés dans ou dans toute la zone. Si la zone est une zone de segment d'accroche, l'une des fonctions de routage externe suivantes peut s'afficher : • Importer des LSA externes : Importe et propage les LSA externes. • N° d'importation LSA : N'importe pas et ne propage pas les LSA externes. Si la zone n'est pas une zone de segment d'accroche, la seule option est Importer aucun LSA.
SPF fonctionne	Nombre de fois que la table de route intra-zone a été calculée à l'aide de la base de données d'état des liens de cette zone. (Ceci est généralement calculé en utilisant l'algorithme de Dijkstra.)

(A continué)

Champ	Description
Nombre de routeurs de bordure de zone	Le nombre total de routeurs de bordure de zone qui sont accessibles à nouveau dans cette zone. Il est initialement nul, et est calculé à chaque passe SPF.
Décompte LSA zone	Nombre d'annonces d'état de lien dans la base de données d'état de lien de cette zone, à l'exclusion DES LSA externes.
Somme de contrôle LSA zone	Somme non signée de 32 bits de la somme de contrôle d'annonce d'état de lien contenue dans la base de données d'état de lien de cette zone. Cette somme exclut les annonces d'état de lien externes (LSA type 5). Vous pouvez utiliser la somme pour déterminer si une modification s'est produite dans la base de données d'état de liaison du commutateur et pour comparer la base de données d'état de liaison de deux unités.
Importer les LSA récapitulatifs	Récapitulatif des LSA importés dans cette zone.

Ajoutez une zone de stub OSPFv3

Une zone de stub est une zone contrôlée qui n'autorise pas les routes externes provenant de l'extérieur du réseau OSPFv3.

Pour ajouter une zone de stub OSPFv3 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **routage > OSPFv3 > Avancé > Configuration de la zone de tronçon**.
La page Configuration de la zone de stub OSPFv3 s'affiche.
6. Dans le champ **ID de zone**, entrez un ID de zone OSPFv3.
Un ID de zone est un entier de 32 bits au format décimal à points qui identifie de manière unique la zone à laquelle une interface est connectée.
7. Dans le menu **Import Summary LSA**, sélectionnez si les LSA récapitulatifs sont importés :
 - Activer. Les LSA récapitulatifs sont importés dans des zones de stub.
 - Désactiver : Les LSA récapitulatifs ne sont pas importés dans les zones de stub.
8. Dans le champ **coût par défaut**, entrez la valeur métrique qui doit être appliquée pour la route par défaut annoncée à la zone de segment d'accroche.
La plage est de 1 à 16 777 215.
9. Cliquez sur le bouton **Add** (Ajouter).
La zone est ajoutée en tant que zone de segment d'accroche.
10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Champ	Description
SPF fonctionne	Nombre de fois que la table de route intra-zone a été calculée à l'aide de la base de données d'état des liens de cette zone. (Ceci est généralement calculé en utilisant l'algorithme de Dijkstra.)
Nombre de routeurs de bordure de zone	Nombre total de routeurs de bordure de zone accessibles dans cette zone. Il est initialement nul, et est calculé à chaque passe SPF.
Décompte LSA zone	Nombre d'annonces d'état de lien dans la base de données d'état de lien de cette zone, à l'exclusion DES LSA externes.
Somme de contrôle LSA zone	Somme non signée de 32 bits de la somme de contrôle d'annonce d'état de lien contenue dans la base de données d'état de lien de cette zone. Cette somme exclut les annonces d'état de lien externes (LSA type 5). Vous pouvez utiliser la somme pour déterminer si une modification s'est produite dans la base de données d'état de liaison du commutateur et pour comparer la base de données d'état de liaison de deux unités.
Type de service	ToS normal associé à la métrique segment d'accroche.

Ajoutez une zone NSSA OSPFv3

La zone OSPFv3 Not-SO-stubby (NSSA) peut recevoir des routes externes (LSA de type 7) et les transférer vers d'autres zones. Vous pouvez choisir si les LSA récapitulatifs (LSA de type 3) peuvent être importés dans des zones de stub.

Pour ajouter une zone NSSA OSPFv3 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **rouage > OSPFv3 > Avancé > Configuration de zone NSSA** .

La page Configuration de la zone NSSA OSPFv3 s'affiche.

6. Dans le champ **ID de zone**, entrez un ID de zone OSPFv3.

Un ID de zone est un entier de 32 bits au format décimal à points qui identifie de manière unique la zone à laquelle une interface est connectée.

7. Dans le menu **Import Summary LSA**, sélectionnez si les LSA récapitulatifs sont importés :

- Activer. Les LSA récapitulatifs sont importés dans des zones de stub.
 - Désactiver : Les LSA récapitulatifs ne sont pas importés dans les zones de stub.
8. Les options de la section Default information Origin du tableau vous permettent de configurer le commutateur pour annoncer une route par défaut dans le NSSA lorsque l'importation des LSA récapitulatifs est désactivée :
- a. Dans le menu **mode Admin**, sélectionnez **Activer** pour laisser le commutateur annoncer une route par défaut ou **désactiver** pour empêcher le commutateur de le faire.
 - b. Dans le champ **valeur métrique**, définissez la valeur métrique de la route par défaut.
La plage est de 1 à 16777214.
 - c. Dans le menu **type de métrique**, sélectionnez le type de métrique à utiliser dans la route par défaut :
 - **Coût comparable** : Métriques externes de type 1 comparables à la métrique OSPFv3
 - **Coût non comparable** : Métriques externes de type 2 supposées supérieures au coût de la métrique OSPFv3.
9. Dans le menu **rôle du traducteur**, sélectionnez le rôle du NSSA :
- **Toujours** : Le commutateur assume le rôle de traducteur lorsque informatique devient un routeur de frontière.
 - **Candidat** : Le commutateur participe au processus d'élection du traducteur lorsque informatique atteint l'état de routeur de frontière.
10. Dans le champ **intervalle de stabilité du traducteur**, entrez la période pendant laquelle le commutateur étend son rôle de traducteur après qu'un autre périphérique devient le traducteur.
La plage est de 0 à 3600 secondes.
11. Dans le menu **mode redistribution**, sélectionnez si les routes externes apprises sont redistribuées :
- Activer. L'ABR de la NSSA distribue les routes externes apprises à la NSSA.
 - Désactiver : L'ABR de la NSSA ne distribue pas les routes externes apprises à la NSSA.
12. Cliquez sur le bouton **Add** (Ajouter).
La zone est ajoutée en tant que zone NSSA.
13. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Champ	Description
SPF fonctionne	Nombre de fois que la table de route intra-zone a été calculée à l'aide de la base de données d'état des liens de cette zone. (Ceci est généralement calculé en utilisant l'algorithme de Dijkstra.)
Nombre de routeurs de bordure de zone	Le nombre total de routeurs de bordure de zone qui sont accessibles à nouveau dans cette zone. Il est initialement nul, et est calculé à chaque passe SPF.
Décompte LSA zone	Nombre d'annonces d'état de lien dans la base de données d'état de lien de cette zone, à l'exclusion DES LSA externes.
Somme de contrôle LSA zone	Somme non signée de 32 bits de la somme de contrôle d'annonce d'état de lien contenue dans la base de données d'état de lien de cette zone. Cette somme exclut les annonces d'état de lien externes (LSA de type 5). Vous pouvez utiliser la somme pour déterminer si une modification s'est produite dans la base de données d'état de liaison du commutateur et pour comparer la base de données d'état de liaison de deux unités.
Etat du traducteur	Ce champ indique si et comment le routeur de frontière NSSA convertit les LSA de type 7 en LSA de type 5 : • Sous tension Le rôle de traducteur du routeur de frontière NSSA est défini sur toujours. • Élus : Le routeur de frontière NSSA candidat traduit les LSA de type 7 en LSA de type 5. • Désactivé : Le routeur de frontière NSSA candidat ne traduit pas les LSA de type 7 en LSA de type 5.

Ajoutez une plage de zones OSPFv3

Vous ajoutez une plage de zones OSPFv3 en définissant un ID de zone avec une plage d'adresses (préfixe IPv6). Vous définissez ensuite également les LSA associés à la zone et si la plage d'adresses est annoncée en dehors de la zone.

Vous pouvez associer une plage de zones OSPFv3 à une zone commune (voir [Ajouter ou supprimer un ID de zone commune OSPFv3](#) à la page 650), une zone de stub (voir [Ajoutez une zone de stub OSPFv3](#) à la page 652) ou une zone NSSA (voir [Ajoutez une zone NSSA OSPFv3](#) à la page 654).

Pour ajouter une plage de zones OSPFv3 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.
4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **routage > OSPFv3 > Avancé > Configuration de la plage de zones**.
La page Configuration de la plage de zones OSPFv3 s'affiche.
6. Dans le champ **ID de zone**, entrez un ID de zone OSPFv3.
Un ID de zone est un entier de 32 bits au format décimal à points qui identifie de manière unique la zone à laquelle une interface est connectée.
7. Dans le champ **préfixe IPv6**, entrez l'adresse IPv6 et le préfixe de la zone sélectionnée.
8. Dans le menu **LSDB type**, sélectionnez le type d'annonces d'état de liaison (LSA) qui doit être associé à l'ID de zone et à la plage d'adresses.
 - **Résumé du réseau** : Le commutateur génère des LSA de résumé du réseau (LSA de type 3) pour la zone. Il s'agit de l'option par défaut.
 - **NSSA externe** : Le commutateur génère des LSA externes NSSA (LSA de type 7) pour la zone. Ces types de LSA fournissent plus d'informations.
9. Dans le menu **annoncer**, sélectionnez si la plage d'adresses est annoncée en dehors de la zone :
 - Activer. La plage d'adresses est annoncée en dehors de la zone via les LSA de résumé du réseau. Il s'agit de l'option par défaut.
 - Désactiver : La plage d'adresses n'est pas annoncée en dehors de la zone.
10. Cliquez sur le bouton **Add** (Ajouter).
L'ID et la plage de zone OSPFv3 sont ajoutés.
11. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez une interface OSPFv3

Vous pouvez configurer une ou plusieurs interfaces OSPFv3, qui sont des interfaces connectées aux zones OSPFv3 via des connexions point à point ou de diffusion.

Pour configurer une interface OSPFv3 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **roulage > OSPFv3 > Avancé > statistiques d'interface**.

La page Configuration de l'interface OSPFv3 s'affiche.

6. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :

- **1 ou ID d'unité pour un commutateur empilé :**

- 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
 - **ID d'unité pour un commutateur empilé** : Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
 - VLAN Seuls les VLAN sont affichés.
 - **Tous**: Les interfaces physiques et les VLAN sont affichés, ou pour une pile de commutateurs, les interfaces physiques et les VLAN de tous les commutateurs sont affichés.
7. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :
- Pour configurer une interface ou un VLAN unique, cochez la case associée à l'interface ou au VLAN, ou tapez le numéro de l'interface ou du VLAN dans le champ **aller à l'interface** et cliquez sur le bouton **aller**.
 - Pour configurer plusieurs interfaces ou VLAN avec les mêmes paramètres, cochez la case associée à chaque interface ou VLAN.
8. Dans le champ **ID de zone**, entrez un ID de zone OSPFv3.
- Un ID de zone est un entier de 32 bits au format décimal à points qui identifie de manière unique la zone à laquelle une interface est connectée.
9. Sélectionnez un bouton radio mode Admin :
- Activer. OSPFv3 est activé pour l'interface.
 - Désactiver : OSPFv3 est désactivé pour l'interface. Il s'agit de l'option par défaut.
- OSPFv3 ne peut devenir opérationnel sur l'interface que si celle-ci est configurée avec une adresse IP et un masque de sous-réseau (voir [Configurer les interfaces de routage IPv6](#) à la page 548).
- Vous pouvez configurer les paramètres OSPFv3 sans activer OSPFv3 sur l'interface, mais la modification ne prend effet que lorsque vous activez OSPFv3 sur l'interface. Les champs suivants s'affichent uniquement si vous activez OSPFv3 sur l'interface : État, routeur désigné, routeur désigné de sauvegarde et nombre d'événements de liaison.
10. Dans le champ **priorité du routeur**, entrez la priorité OSPFv3 de l'interface.
- Il s'agit d'un nombre compris entre 0 et 255. La valeur par défaut est 1, qui est la priorité la plus élevée du routeur. La valeur 0 indique que le routeur n'est pas éligible pour devenir le routeur désigné sur ce réseau.
11. Dans le champ **intervalle de retransmission**, entrez le nombre de secondes entre les annonces d'état de liaison pour les contiguïtés, c'est-à-dire pour les périphériques voisins qui forment une contiguïté OSPFv3 avec l'interface.

L'intervalle est également utilisé lors de la retransmission de descriptions de base de données et de paquets de demande d'état de liens. La valeur de l'intervalle est comprise entre 1 et 3600 secondes (1 heure). La valeur par défaut est de 5 secondes.

12. Dans le champ **intervalle Hello**, entrez l'intervalle Hello OSPFv3 pour l'interface.

Cet intervalle doit être le même pour tous les routeurs et commutateurs du réseau. L'intervalle est compris entre 1 et 65 535 secondes. La valeur par défaut est 10 secondes.

13. Dans le champ **intervalle mort**, entrez le nombre de secondes pendant lesquelles l'interface attend les paquets Hello d'un voisin avant de déterminer que ce voisin est en panne.

Cet intervalle doit être le même pour tous les routeurs et commutateurs du réseau. Cet intervalle doit être un multiple de l'intervalle Hello. L'intervalle est compris entre 1 et 65 535. La valeur par défaut est de 40 secondes. (L'intervalle Hello par défaut est de 10 secondes.)

14. Dans le champ **lfransit Delay Interval**, entrez le nombre estimé de secondes nécessaires pour transmettre un paquet de mise à jour de l'état de la liaison sur l'interface.

L'intervalle est compris entre 1 et 3600 secondes (1 heure). La valeur par défaut est 1 seconde.

15. Dans le menu **ignorer MTU**, sélectionnez si la détection de discordance MTU OSPFv3 est désactivée :

- Activer. La détection des discordances MTU OSPFv3 est *désactivée* sur les paquets de description de base de données entrants. La valeur par défaut est Disable (désactiver) (la détection des discordances MTU est activée).
- Désactiver : La détection des discordances MTU OSPFv3 est *activée* sur les paquets de description de base de données entrants. Il s'agit de l'option par défaut.

16. Dans le menu **mode passif**, sélectionnez si l'interface ne forme pas de contiguïté :

- Activer. L'interface est passive pour empêcher OSPFv3 de former une contiguïté. OSPFv3 annonce les réseaux attachés à des interfaces passives comme des réseaux stub.
- Désactiver : L'interface n'est pas passive et OSPFv3 peut former une contiguïté. Il s'agit de l'option par défaut.

17. Dans le menu **type de réseau**, sélectionnez le type de réseau OSPFv3 pour l'interface :

- Diffusion L'interface peut se connecter à plusieurs routeurs OSPFv3. Il s'agit de l'option par défaut.
- **Point à point** : L'interface peut se connecter à un autre routeur OSPFv3.

18. Dans le champ **coût métrique**, entrez la valeur utilisée par OSPFv3 pour calculer les chemins les plus courts.

La plage est de 1 à 65 535. Le numéro par défaut est 1.

19. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

20. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Champ	Description
Adresse IPv6	Adresse IP de l'interface.
Intervalle d'accusé de réception LSA	Nombre de secondes que l'interface doit attendre avant d'envoyer un accusé de réception retardé.
Etat	État de l'interface OSPFv3 : inactif Il s'agit de l'état initial de l'interface. L'interface n'est pas utilisable pour OSPFv3, et les paramètres d'interface sont à leurs valeurs initiales. Toutes les minuteriers d'interface sont désactivées et aucune contiguïté n'est associée à l'interface. Bouclage : L'interface est rebouclée dans le matériel ou le logiciel. L'interface n'est pas disponible pour le trafic de données régulier. Vous pouvez obtenir des informations sur l'interface en envoyant des ping ICMP à l'interface ou via un test d'erreur de bit car les paquets IP peuvent toujours être adressés à une interface dans un état de bouclage. Une interface dans un état de bouclage est annoncée dans des LSA comme route hôte unique pour laquelle la destination est l'adresse de l'interface IP. PATIENTEZ ! Le commutateur surveille les paquets Hello reçus afin de détecter l'identité du routeur désigné de secours pour le réseau. Le commutateur ne peut pas sélectionner un routeur désigné de secours ou un routeur désigné tant que le informatique n'est pas sorti de l'état d'attente. Cela évite les modifications inutiles du routeur désigné de sauvegarde. Routeur désigné : Le commutateur est le routeur désigné sur le réseau connecté. Des contiguïtés sont établies avec tous les autres routeurs et commutateurs du réseau. Le commutateur doit également émettre un LSA de réseau pour le nœud de réseau. Le réseau LSA contient des liens vers tous les commutateurs et routeurs (y compris le routeur désigné) du réseau. Routeur désigné de sauvegarde : Le commutateur est le routeur désigné de secours sur le réseau connecté. Le commutateur est promu au rang de routeur désigné si le routeur désigné actuel tombe en panne. Le commutateur établit des contiguïtés à tous les autres routeurs connectés au réseau. Le routeur désigné de sauvegarde exécute des fonctions légèrement différentes lors de l'inondation LSA, par rapport au routeur désigné. Autre routeur désigné : L'interface est connectée à une diffusion sur laquelle d'autres routeurs sont le routeur désigné et le routeur désigné de secours. Le commutateur tente de former des contiguïtés au routeur désigné et au routeur désigné de secours.
Routeur désigné	Identité du routeur désigné pour ce réseau, telle qu'elle est détectée par le routeur publicitaire. Le routeur désigné est identifié par son ID de routeur. La valeur 0.0.0.0 signifie qu'aucun routeur désigné n'est détecté.

(A continué)

Champ	Description
Routeur désigné de sauvegarde	Identité du routeur désigné de sauvegarde pour ce réseau, telle qu'elle est détectée par le routeur publicitaire. Le routeur désigné de sauvegarde est identifié par son ID de routeur. La valeur 0.0.0.0 signifie qu'aucun routeur désigné de sauvegarde n'est détecté.
Nombre d'événements Link	Nombre de fois que l'interface OSPFv3 a changé d'état.

Afficher ou effacer les statistiques OSPFv3 pour une interface

Si OSPFv3 est activé, vous pouvez afficher ou effacer les statistiques OSPFv3 pour une interface.

Pour afficher ou effacer les statistiques OSPFv3 d'une interface :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **rouage > OSPFv3 > Avancé > statistiques d'interface**.

La page statistiques de l'interface OSPFv3 s'affiche.

6. Dans le menu **interface**, sélectionnez l'interface.
7. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).
8. Pour effacer tous les compteurs et réinitialiser toutes les statistiques de l'interface OSPFv3 aux valeurs par défaut, cliquez sur le bouton **Effacer**.
9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Champ	Description
ID zone OSPFv3	Zone OSPFv3 à laquelle appartient l'interface. Un ID de zone OSPFv3 est un entier de 32 bits au format décimal à points qui identifie de manière unique la zone à laquelle l'interface se connecte.
Nombre de routeurs de bordure de zone	Le nombre de routeurs de bordure de zone (ABR) accessibles dans cette zone. Il est initialement nul et calculé à chaque passage SPF (Shortest Path First).
Nombre DE routeurs de bordure	Nombre total de routeurs périphériques de système autonome (AS) accessibles dans cette zone. Il est initialement nul, et est calculé à chaque passe SPF.
Décompte LSA zone	Nombre d'annonces d'état de lien dans la base de données d'état de lien de cette zone, à l'exclusion DES LSA externes.
Adresse IPv6	Adresse IPv6 de l'interface.
Événements d'interface	Nombre de fois que l'interface OSPFv3 a changé d'état ou qu'une erreur s'est produite.
Événements virtuels	Nombre de changements d'état ou d'erreurs survenus sur ce lien virtuel.
Événements voisins	Nombre de fois que cette relation de voisin a changé d'état ou qu'une erreur s'est produite.
Paquets envoyés :	Nombre de paquets OSPFv3 transmis sur l'interface.
Paquets reçus :	Nombre de paquets OSPFv3 valides reçus sur l'interface.
ABANDONNER	Nombre de paquets OSPFv3 reçus rejetés en raison d'une erreur dans le paquet ou d'une erreur dans le traitement du paquet.
Version incorrecte	Nombre de paquets OSPFv3 reçus pour lesquels le champ version de l'en-tête OSPFv3 ne correspond pas à la version du processus OSPFv3 qui traite le paquet.
Lien virtuel introuvable	Nombre de paquets OSPFv3 reçus rejetés parce que l'interface d'entrée se trouve dans une zone non dorsale et que l'en-tête OSPFv3 a identifié le paquet comme appartenant au dorsal, mais qu'OSPFv3 n'a pas de lien virtuel avec l'expéditeur du paquet.
Discordance de zone	Nombre de paquets OSPFv3 rejetés car l'ID de zone dans l'en-tête OSPFv3 n'est pas l'ID de zone configuré sur l'interface d'entrée.

(A continué)

Champ	Description
Adresse IP de destination non valide.	Nombre de paquets OSPFv3 rejetés car l'adresse IP de destination du paquet n'est pas l'adresse de l'interface d'entrée et n'est pas l'adresse multicast <i>AllDrouters</i> ou <i>AllSpfRouters</i> .
Aucun voisin à l'adresse source	Nombre de paquets OSPFv3 abandonnés parce que l'expéditeur n'est pas un voisin existant ou que l'adresse IP de l'expéditeur ne correspond pas à l'adresse IP enregistrée précédemment pour ce voisin.
Type de paquet OSPF non valide	Nombre de paquets OSPFv3 rejetés car le champ type de paquet dans l'en-tête OSPFv3 n'est pas un type connu.
Hellos ignoré	Nombre de paquets Hello reçus ignorés par l'interface. Ce sont les paquets Hello des nouveaux voisins après que la limite a été atteinte pour le nombre de voisins sur l'interface ou sur le commutateur.
Hellos envoyés	Nombre de paquets Hello envoyés sur l'interface.
Hellos reçus	Nombre de paquets Hello reçus sur l'interface.
Paquets DD envoyés	Nombre de paquets DD (Database description) envoyés sur l'interface.
Paquets DD reçus	Nombre de paquets de description de base de données reçus sur l'interface.
Demandes LS envoyées	Nombre de requêtes d'état de liaison (LS) envoyées sur l'interface.
Demandes LS reçues	Nombre de demandes d'état de liaison reçues sur l'interface.
Mises à jour LS envoyées	Nombre de mises à jour de l'état de la liaison envoyées sur l'interface.
Mises à jour LS reçues	Nombre de mises à jour de l'état de la liaison reçues sur l'interface.
Accusés de réception LS envoyés	Nombre d'accusés de réception d'état de liaison envoyés sur l'interface.
Accusés de réception LS reçus	Nombre d'accusés de réception d'état de liaison reçus sur l'interface.

Afficher ou effacer les informations de voisinage OSPFv3 pour une interface

Si OSPFv3 est activé, vous pouvez afficher les voisins OSPFv3. Vous pouvez également effacer les informations de voisinage OSPFv3.

Pour afficher ou effacer les informations de voisinage OSPFv3 pour une interface :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > OSPFv3 > Avancé > table de voisinage**.

La page table de voisinage OSPFv3 s'affiche.

6. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).
7. Pour effacer les informations de voisinage OSPFv3, en rétablissant les valeurs par défaut des champs de la table, cliquez sur le bouton **Effacer**.
8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Champ	Description
Interface	Interface pour laquelle les données sont affichées.
Identifiant d'interface	ID d'interface que l'interface du routeur voisin annonce dans ses paquets Hello.
Code ID du routeur	Entier de 32 bits au format décimal à points qui représente l'interface voisine.
ID zone	ID de zone de la zone OSPFv3 associée à l'interface.

(A continué)

Champ	Description
Options	Valeur entière qui indique les capacités optionnelles OSPFv3 prises en charge par le voisin. Les capacités optionnelles OSPFv3 du voisin sont également répertoriées dans ses paquets Hello. Les informations Options permettent de rejeter les paquets Hello reçus en cas de non-concordance dans certaines capacités OSPFv3. (Si les paquets Hello sont rejetés, par exemple, les relations de voisinage ne peuvent pas être formées.)
Priorité du routeur	Priorité OSPFv3 pour l'interface. La priorité d'une interface est un entier de priorité compris entre 0 et 255. La valeur 0 indique que le routeur n'est pas éligible pour devenir le routeur désigné sur ce réseau.
Etat	L'état du voisin OSPD : inactif Il s'agit de l'état initial d'une conversation de voisinage. Il indique qu'aucune information récente n'a été reçue du voisin. Sur les réseaux à accès multiple non diffusé (NBMA), les paquets Hello peuvent toujours être envoyés aux voisins à l'état inactif, bien qu'à une fréquence réduite. Tentative: Cet état n'est valide que pour les voisins connectés à des réseaux NBMA. Il indique qu'aucune information récente n'a été reçue du voisin, mais qu'un effort plus concerté doit être fait pour contacter le voisin. Cela se fait en envoyant les paquets Hello voisins à intervalles Hello. Init Un paquet Hello a récemment été détecté en provenance du voisin. Cependant, la communication bidirectionnelle n'est pas encore établie avec le voisin (par exemple, le routeur n'est pas inclus dans le paquet Hello du voisin). Tous les voisins dans cet état ou dans un état listé ci-dessous dans ce tableau sont inclus dans les paquets Hello envoyés depuis l'interface associée. 2 voies: La communication entre les deux interfaces de routage est bidirectionnelle. Ceci est assuré par le fonctionnement du protocole Hello. Il s'agit de l'état le plus avancé à moins de commencer l'établissement de la contiguïté. Le routeur désigné de sauvegarde est sélectionné parmi l'ensemble de voisins dans l'état bidirectionnel ou un état répertorié ci-dessous dans ce tableau. Début d'échange : Il s'agit de la première étape de la création d'une contiguïté entre les deux interfaces de routage voisines. Le processus dans cet état détermine quel routeur est le maître et quel est le numéro de séquence DD initial. Les conversations voisines dans cet état ou dans un état répertorié ci-dessous dans ce tableau sont appelées contiguïtés. Échange: Les interfaces de routage incluent toute sa base de données d'état de liens dans des paquets de description de base de données qu'elle envoie au voisin. Le routeur peut également envoyer des paquets de demande d'état de liaison pour demander les LSA les plus récents du voisin. Toutes les contiguïtés dans l'état Exchange ou dans un état répertorié ci-dessous dans ce tableau sont utilisées par la procédure d'inondation. Ces contiguïtés peuvent transmettre et recevoir tous les types de paquets de protocole de routage OSPFv3. Chargement Les paquets de demande d'état de liaison sont envoyés au voisin demandant les LSA les plus récents qui ont été découverts mais pas encore reçus dans l'état Exchange. Complet: Les routeurs voisins sont entièrement adjacents. Ces contiguïtés sont désormais incluses dans les LSA de routeur et les LSA de réseau.
Temps mort	Durée en secondes pendant laquelle le commutateur attend avant de déterminer que le voisin est inaccessible.

(A continué)

Champ	Description
Événements	Nombre de fois que cette relation de voisin a changé d'état ou qu'une erreur s'est produite.
Longueur de la file d'attente de retransmission	Entier représentant la longueur actuelle de la file d'attente de retransmission de l'ID de routeur voisin spécifié de l'interface spécifiée.

Affichez la base de données d'état des liens OSPFv3

Si OSPFv3 est activé, vous pouvez afficher la base de données d'état des liens OSPFv3.

Pour afficher la base de données d'état des liens OSPFv3 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > OSPFv3 > Avancé > base de données d'état des liens** .

La page affiche les sections base de données d'état de liaison OSPFv3 et table LSDB externe OSPFv3.

Le terme LSDB signifie Link State Database.

6. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

Les tableaux suivants décrivent les champs en lecture seule de la page.

Table 126 : Base de données d'état de liaison OSPFv3

Champ	Description
Code ID du routeur	Nombre de 32 bits au format décimal à points qui identifie le commutateur dans le système autonome (AS). Pour modifier l'ID du routeur, vous devez d'abord désactiver OSPFv3. Après avoir défini un nouvel ID de routeur, vous devez réactiver OSPFv3 pour que la modification prenne effet. La valeur par défaut est 0,0,0, bien qu'il ne s'agisse pas d'un ID de routeur valide.
ID zone	ID de la zone OSPFv3 à laquelle l'une des interfaces de commutateur est connectée. Un ID de zone est un entier de 32 bits au format décimal à points qui identifie de manière unique la zone à laquelle une interface est connectée.
Type de LSA	Le format et la fonction de l'annonce d'état de lien: • Routeur LSA : Un routeur peut émettre un ou plusieurs LSA de routeur pour une zone. Un LSA de routeur provient d'une zone et décrit les états collectés de toutes les interfaces du routeur connectées à la zone. • Réseau LSA: Un réseau LSA est émis par le routeur désigné pour chaque liaison à laquelle deux routeurs ou plus sont rattachés. Le LSA répertorie tous les routeurs rattachés à la liaison. • Routeur inter-zone LSA: Ce type de LSA provient d'un routeur de bordure de zone (ABR) et décrit un préfixe externe à la zone, mais interne au système autonome (AS). • AS-externe LSA: Ce type de LSA provient d'un routeur de frontière de système autonome (ASBR) et décrit un chemin vers un préfixe externe au système autonome (AS). • Lien LSA: Un routeur émet une liaison LSA distincte pour chaque liaison rattachée. Il fournit l'adresse locale du lien du routeur aux routeurs qui sont attachés au lien ainsi qu'une liste de préfixes IPv6 qui peuvent être associés au lien. • Préfixe intra-zone LSA: Le routeur désigné d'une liaison émet un ou plusieurs LSA de préfixe intra-zone pour annoncer les préfixes de la liaison dans toute la zone. Un routeur peut émettre plusieurs LSA de préfixe intra-zone pour une zone afin d'annoncer ses propres préfixes et ceux de ses liaisons de souche rattachées.
ID LS	L'ID d'état de liaison identifie la partie du domaine de routage décrite par l'annonce. La valeur de l'ID LS dépend du type LS de la publicité.
Age :	Temps en secondes écoulé depuis que l'annonce d'état de lien a été émise pour la première fois.
Séquence	Entier de 32 bits signé utilisé pour détecter les annonces d'état de lien anciennes et dupliquées. Plus le numéro de séquence est grand, plus la publicité est récente.

Table 126 : Base de données d'état de liaison OSPFv3 (A continué)

Champ	Description
Total de contrôle	Somme de contrôle du contenu complet de la publicité, à l'exception du champ LS Age. La somme de contrôle est utilisée pour détecter la corruption de données d'une publicité. Cette corruption peut se produire lorsqu'une publicité est inondée ou lorsqu'elle est conservée dans la mémoire d'un routeur.
Options	Le champ Options de l'en-tête annonce état de lien indique les fonctionnalités facultatives associées à l'annonce : • Q: Active la prise en charge de l'ingénierie du trafic QoS. • E Spécifie la manière DONT les LSA externes sont inondés. • MC Spécifie la manière dont les datagrammes de multidiffusion IP sont transmis conformément aux spécifications standard. • O: Spécifie si les LSA opaques sont pris en charge. • v Spécifie si les extensions OSPF pour classe de service (cos) et VPN sont prises en charge.
Options du routeur	Le champ Options du routeur dans l'en-tête d'annonce d'état de lien indique le type de routeur OSPFv3 associé à l'annonce : • Bit V: Le routeur est un point d'extrémité d'une ou plusieurs liaisons virtuelles entièrement adjacentes pour lesquelles la zone décrite est la zone de transit. (V signifie point de terminaison de liaison virtuelle.) • Bit E: Le routeur est un routeur de limite AS. (E signifie externe.) • Bit B: Le routeur est un routeur de bordure de zone. (B signifie bordure.) • Bit NT: Le routeur est un routeur de frontière NSSA qui traduit inconditionnellement les NSSA-LSA en AS-External-LSA. (NT signifie traduction NSSA.) Cela signifie que le routeur a sa configuration de zone de rôle de traducteur NSSA définie sur toujours.

Table 127 : Base de données LSA externe OSPFv3

Champ	Description
Code ID du routeur	Nombre de 32 bits au format décimal à points qui identifie le commutateur dans le système autonome (AS). Pour modifier l'ID du routeur, vous devez d'abord désactiver OSPFv3. Après avoir défini un nouvel ID de routeur, vous devez réactiver OSPFv3 pour que la modification prenne effet. La valeur par défaut est 0,0,0,0, bien qu'il ne s'agisse pas d'un ID de routeur valide.
Type de LSA	Le format et la fonction de l'annonce d'état de lien: • Routeur LSA : Un routeur peut émettre un ou plusieurs LSA de routeur pour une zone. Un LSA de routeur provient d'une zone et décrit les états collectés de toutes les interfaces du routeur connectées à la zone. • Réseau LSA: Un réseau LSA est émis par le routeur désigné pour chaque liaison à laquelle deux routeurs ou plus sont rattachés. Le LSA répertorie tous les routeurs rattachés à la liaison. • Routeur inter-zone LSA: Ce type de LSA provient d'un routeur de bordure de zone (ABR) et décrit un préfixe externe à la zone, mais interne au système autonome (AS). • AS-externe LSA: Ce type de LSA provient d'un routeur de frontière de système autonome (ASBR) et décrit un chemin vers un préfixe externe au système autonome (AS). • Lien LSA: Un routeur émet une liaison LSA distincte pour chaque liaison rattachée. Il fournit l'adresse locale du lien du routeur aux routeurs qui sont attachés au lien ainsi qu'une liste de préfixes IPv6 qui peuvent être associés au lien. • Préfixe intra-zone LSA: Le routeur désigné d'une liaison émet un ou plusieurs LSA de préfixe intra-zone pour annoncer les préfixes de la liaison dans toute la zone. Un routeur peut émettre plusieurs LSA de préfixe intra-zone pour une zone afin d'annoncer ses propres préfixes et ceux de ses liaisons de souche rattachées.
ID LS	L'ID d'état de liaison identifie la partie du domaine de routage décrite par l'annonce. La valeur de l'ID LS dépend du type LS de la publicité.
Age :	Temps en secondes écoulé depuis que l'annonce d'état de lien a été émise pour la première fois.
Séquence	Entier de 32 bits signé utilisé pour détecter les annonces d'état de lien anciennes et dupliquées. Plus le numéro de séquence est grand, plus la publicité est récente.
Total de contrôle	Somme de contrôle du contenu complet de la publicité, à l'exception du champ LS Age. La somme de contrôle est utilisée pour détecter la corruption de données d'une publicité. Cette corruption peut se produire lorsqu'une publicité est inondée ou lorsqu'elle est conservée dans la mémoire d'un routeur.

Configurez une liaison virtuelle OSPFv3

Si vous ne pouvez pas configurer une liaison physique entre le commutateur et la zone de backbone OSPFv3, vous pouvez ajouter une liaison virtuelle pour vous connecter à la zone de backbone via une zone commune (non-backbone). Vous pouvez configurer une liaison virtuelle entre tous les routeurs de bordure de zone qui ont des interfaces physiques avec la zone commune.

Pour configurer un lien virtuel OSPFv3 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routing > OSPFv3 > Avancé > Configuration de liaison virtuelle**.

La page Configuration de liaison virtuelle OSPFv3 s'affiche.

6. Dans le champ **ID de zone**, entrez un ID de zone OSPFv3.

Un ID de zone est un entier de 32 bits au format décimal à points qui identifie de manière unique la zone à laquelle une interface est connectée.

7. Dans le champ **ID du routeur voisin**, entrez la partie voisine d'une spécification de lien virtuel.

8. Dans le champ **intervalle Hello**, entrez l'intervalle Hello OSPFv3 pour l'interface.

Cet intervalle doit être le même pour tous les routeurs et commutateurs du réseau. L'intervalle est compris entre 1 et 65 535 secondes. La valeur par défaut est 10 secondes.

9. Dans le champ **intervalle mort**, entrez le nombre de secondes pendant lesquelles l'interface attend les paquets Hello d'un voisin avant de déterminer que ce voisin est en panne.

Cet intervalle doit être le même pour tous les routeurs et commutateurs du réseau. Cet intervalle doit être un multiple de l'intervalle Hello. L'intervalle est compris entre 1 et 65 535. La valeur par défaut est de 40 secondes. (L'intervalle Hello par défaut est de 10 secondes.)

10. Dans le champ **Iftransit Delay Interval**, entrez le nombre estimé de secondes nécessaires pour transmettre un paquet de mise à jour de l'état de la liaison sur l'interface.

L'intervalle est compris entre 1 et 3600 secondes (1 heure). La valeur par défaut est 1 seconde.

11. Dans le champ **intervalle de retransmission**, entrez le nombre de secondes entre les annonces d'état de liaison pour les contiguïtés, c'est-à-dire pour les périphériques voisins qui forment une contiguïté OSPFv3 avec l'interface.

L'intervalle est également utilisé lors de la retransmission de descriptions de base de données et de paquets de demande d'état de liens. La valeur de l'intervalle est comprise entre 1 et 3600 secondes (1 heure). La valeur par défaut est de 5 secondes.

12. Cliquez sur le bouton **Add** (Ajouter).

Les paramètres sont enregistrés.

13. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Champ	Description
Etat voisin	
État de l'interface voisine OSPFv3 :	
	inactif Il s'agit de l'état initial de l'interface. L'interface n'est pas utilisable pour OSPFv3, et les paramètres d'interface sont à leurs valeurs initiales. Toutes les minuteries d'interface sont désactivées et aucune contiguïté n'est associée à l'interface.
	Bouclage : L'interface est rebouclée dans le matériel ou le logiciel. L'interface n'est pas disponible pour le trafic de données régulier. Vous pouvez obtenir des informations sur l'interface en envoyant des ping ICMP à l'interface ou via un test d'erreur de bit car les paquets IP peuvent toujours être adressés à une interface dans un état de bouclage. Une interface dans un état de bouclage est annoncée dans des LSA comme route hôte unique pour laquelle la destination est l'adresse de l'interface IP.
	PATIENTEZ ! Le dispositif voisin surveille les paquets Hello reçus afin de détecter l'identité du routeur désigné de secours pour le réseau. Le périphérique voisin ne peut pas sélectionner un routeur désigné de secours ou un routeur désigné tant que informatique n'est pas sorti de l'état d'attente. Cela évite les modifications inutiles du routeur désigné de sauvegarde.
	Routeur désigné : Le périphérique voisin est le routeur désigné sur le réseau connecté. Des contiguïtés sont établies avec tous les autres routeurs et commutateurs du réseau. Le périphérique voisin doit également émettre un LSA de réseau pour le nœud de réseau. Le réseau LSA contient des liens vers tous les commutateurs et routeurs (y compris le routeur désigné) du réseau.

(A continué)

Champ	Description
	Routeur désigné de sauvegarde : Le périphérique voisin est le routeur désigné de sauvegarde sur le réseau connecté. Le périphérique voisin est promu au rang de routeur désigné si le routeur désigné actuel tombe en panne. Le dispositif voisin établit des contiguïtés à tous les autres routeurs reliés au réseau. Le routeur désigné de sauvegarde exécute des fonctions légèrement différentes lors de l'inondation LSA, par rapport au routeur désigné.
	Autre routeur désigné : L'interface est connectée à une diffusion sur laquelle d'autres routeurs sont le routeur désigné et le routeur désigné de secours. Le périphérique voisin tente de former des contiguïtés à la fois avec le routeur désigné et le routeur désigné de secours.
Etat	L'état de l'interface du commutateur OSPFv3 : inactif Il s'agit de l'état initial de l'interface. L'interface n'est pas utilisable pour OSPFv3, et les paramètres d'interface sont à leurs valeurs initiales. Toutes les minuteries d'interface sont désactivées et aucune contiguïté n'est associée à l'interface. Bouclage : L'interface est rebouclée dans le matériel ou le logiciel. L'interface n'est pas disponible pour le trafic de données régulier. Vous pouvez obtenir des informations sur l'interface en envoyant des ping ICMP à l'interface ou via un test d'erreur de bit car les paquets IP peuvent toujours être adressés à une interface dans un état de bouclage. Une interface dans un état de bouclage est annoncée dans des LSA comme route hôte unique pour laquelle la destination est l'adresse de l'interface IP. PATIENTEZ ! Le commutateur surveille les paquets Hello reçus afin de détecter l'identité du routeur désigné de secours pour le réseau. Le commutateur ne peut pas sélectionner un routeur désigné de secours ou un routeur désigné tant que le informatique n'est pas sorti de l'état d'attente. Cela évite les modifications inutiles du routeur désigné de sauvegarde. Routeur désigné : Le commutateur est le routeur désigné sur le réseau connecté. Des contiguïtés sont établies avec tous les autres routeurs et commutateurs du réseau. Le commutateur doit également émettre un LSA de réseau pour le nœud de réseau. Le réseau LSA contient des liens vers tous les commutateurs et routeurs (y compris le routeur désigné) du réseau. Routeur désigné de sauvegarde : Le commutateur est le routeur désigné de secours sur le réseau connecté. Le commutateur est promu au rang de routeur désigné si le routeur désigné actuel tombe en panne. Le commutateur établit des contiguïtés à tous les autres routeurs connectés au réseau. Le routeur désigné de sauvegarde exécute des fonctions légèrement différentes lors de l'inondation LSA, par rapport au routeur désigné. Autre routeur désigné : L'interface est connectée à une diffusion sur laquelle d'autres routeurs sont le routeur désigné et le routeur désigné de secours. Le commutateur tente de former des contiguïtés au routeur désigné et au routeur désigné de secours.
Métrique	Valeur métrique utilisée par le lien virtuel pour calculer les chemins les plus courts.

Configurez la redistribution de route OSPFv3

La redistribution de route (RR) permet au commutateur de partager des informations de routage entre des routeurs connectés localement (ou des interfaces de routage) et des informations sur les routes statiques.

Pour configurer la redistribution de route OSPFv3 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > OSPFv3 > Avancé > redistribution de route**.

La page redistribution de route OSPFv3 s'affiche.

6. En regard du champ **source**, cochez la case correspondant à un ou plusieurs types de routes sources auxquels la configuration s'applique :

- Connecté Routes entre les routeurs connectés localement (ou interfaces de routage).
- Statique Routes configurées manuellement.

7. Dans le menu **redistribuer**, sélectionnez si la redistribution est activée :

- Activer. Le type de route peut être redistribué.
- Désactiver : Le type de route ne peut pas être redistribué.

8. Dans le champ **valeur métrique**, définissez la valeur métrique du type de route.

Si le type de route est préconfiguré, la valeur métrique s'affiche, mais vous pouvez modifier informatique. La plage est de 0 à 16777214.

9. Dans le menu **type de métrique**, sélectionnez le type de métrique à utiliser pour le type de route :
 - **Externe type 1** : Métriques externes de type 1 comparables à la métrique OSPFv3.
 - **Externe type 2** : Métriques externes de type 2 supposées supérieures au coût de la métrique OSPFv3.
10. Dans le champ **balise**, définissez la balise du type de route.

Si le type de route est préconfiguré, la balise s'affiche, mais vous pouvez modifier informatique. La plage est de 0 à 4294967295.
11. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.
12. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurer le transfert non-stop OSPFv3

Le transfert non-stop (NSF) OSPFv3 garantit que le routage OSPF se poursuit en laissant temporairement d'autres périphériques du réseau effectuer le routage OSPFv3 pour le commutateur. Cela signifie que même si le commutateur redémarre, le routage OSPFv3 peut continuer. (Nous appelons ce type de processus de redémarrage un redémarrage normal.)

Pour configurer OSPFv3 NSF :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > OSPFv3 > Avancé > Récapitulatif NSF OSPFv3**.

La page Récapitulatif NSF OSPFv3 s'affiche.

6. Dans le menu **mode support**, sélectionnez la manière dont le commutateur effectue un redémarrage normal :

- **Toujours**: OSPFv3 effectue un redémarrage progressif pour tous les événements de redémarrage à chaud planifiés et non planifiés.
- Désactivé : Les redémarrages progressifs OSPFv3 sont désactivés. Il s'agit de la sélection par défaut.
- **Planifié** : OSPFv3 n'effectue un redémarrage normal que si un redémarrage est planifié (par exemple, parce qu'une commande CLI est exécutée).

7. Dans le champ **intervalle de redémarrage**, entrez le temps que le commutateur attend après un redémarrage normal avant de poursuivre le routage OSPFv3.

La plage est de 0 à 1800 secondes. La valeur par défaut est de 120 secondes.

8. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Champ	Description
Etat de redémarrage	L'état de redémarrage du mode de prise en charge de l'assistant OSPFv3 : • Ne redémarre pas • Redémarrage planifié • Redémarrage non planifié
Âge de redémarrage (secondes)	Temps en secondes écoulé depuis le dernier redémarrage.
Motif de sortie du redémarrage	Affiche le dernier démarrage du processus de routage OSPFv3 sur le commutateur : • Non tenté : Aucune tentative de redémarrage normal n'a été effectuée. • Progression Un redémarrage normal est en cours. • Terminé Le redémarrage normal précédent s'est terminé avec succès. • Délai expiré : Le délai du redémarrage normal précédent a expiré. • Topologie modifiée : Le redémarrage progressif précédent s'est terminé prématurément en raison d'une modification de topologie.

7

Configurer le routage multidiffusion

Ce chapitre aborde les sujets suivants :

- Routage multicast IPv4 et table de routage multicast IPv4
- Protocole DVMRP (Distance Vector Multicast Routing)
- IGMP pour le routage multicast IPv4
- PIM pour le routage multicast IPv4
- Routes de multidiffusion statiques pour les adresses IPv4
- Limites d'administration multicast pour les adresses IPv4
- Routage multicast IPv6 et table de routage multicast IPv6
- PIM pour le routage multicast IPv6
- MLD pour le routage multicast IPv6
- Routes de multidiffusion statiques pour les adresses IPv6

Routage multicast IPv4 et table de routage multicast IPv4

La multidiffusion est particulièrement adaptée au trafic vidéo et audio nécessitant un contrôle des paquets de multidiffusion pour un fonctionnement optimal. La multidiffusion pour IPv4 inclut la prise en charge d'IGMPv1, IGMPv2 et IGMPv3. La communication de point à multipoint est appelée multidiffusion. L'hôte source (point) transmet un message à un groupe de zéro hôte ou plus (multipoint) identifiés par une adresse de destination IPv4 unique. Bien que la tâche puisse être accomplie en envoyant des messages unicast (point à point) à chacun des hôtes de destination, la multidiffusion est la méthode préférée pour ce type de transmission. Un message de multidiffusion est remis à tous les membres de son groupe d'hôtes de destination avec la même fiabilité que les messages IPv4 monodiffusion réguliers. Il n'est pas garanti que le message arrive intact à tous les membres du groupe de destination ou dans le même ordre par rapport aux autres messages.

Affichez la table de routage multicast IPv4

La table de routage multicast (Mroute) comprend des informations sur l'adresse IPv4 source, les adresses IPv4 de destination du groupe, les interfaces entrante et sortante, les sauts suivants vers lesquels le paquet IPv4 doit être transféré et les protocoles pris en charge.

Pour afficher la table Mroute IPv4 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **roulage > Multicast > table Mroute**.

La page table Mroute s'affiche.

6. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

Le tableau suivant décrit les champs en lecture seule de la page.

Table 128 : Informations de table Mroute IPv4 multicast

Champ	Description
IP du groupe	Adresse IPv4 du groupe de destination.
Adresse IP source	Adresse IPv4 de la source de paquets multicast à combiner avec le groupe IPv4 pour identifier complètement une route unique.
Interface entrante	Interface entrante sur laquelle arrivent les paquets multicast pour cette source/ce groupe.
Interfaces sortantes	Liste des interfaces sortantes sur lesquelles les paquets multicast pour cette source/ce groupe sont transmis.
Temps de fonctionnement (hh:mm:ss)	Temps en secondes depuis la création de l'entrée.
Heure d'expiration (hh:mm:ss)	Temps en secondes avant que cette entrée ne vieillisse et ne soit supprimée du tableau.
Voisin RPF	Adresse IPv4 du voisin RPF (reverse path Forward).
Protocole	Protocole de routage multicast qui a créé dynamiquement cette entrée. Les valeurs possibles sont les suivantes : • PIM-DM • PIM-SM
flag	La valeur affichée dans ce champ est valide si le protocole de routage multicast est PIM-SM. Les valeurs possibles sont RPT et SPT. Pour les autres protocoles, un "-----" est affiché.

Ajoutez des entrées de multidiffusion statiques à la table Mroute IPv4

Vous pouvez ajouter une entrée de multidiffusion statique à la table Mroute IPv4.

Pour ajouter une entrée de multidiffusion statique à la table Mroute IPv4 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **roulage > Multicast > Configuration Mroute Static-Multicast** .

La page Configuration Mroute Static-Multicast s'affiche.

6. Dans le champ **IP du groupe**, spécifiez l'adresse IP du groupe de multidiffusion.
7. Dans le champ **liste des VLAN de sortie**, spécifiez le ou les VLAN auxquels appartient l'adresse IP du groupe de multidiffusion.
8. Cliquez sur le bouton **Add** (Ajouter).

Les paramètres sont enregistrés. L'entrée multicast est ajoutée.

9. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).
10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 129 : Informations de configuration de multidiffusion statique Mroute

Champ	Description
Nombre maximal d'adresses statiques de multidiffusion	Nombre maximal d'adresses multidiffusion statiques que la table Mroute peut contenir.
Nombre actuel d'adresses statiques de multidiffusion	Nombre d'adresses multidiffusion statiques que vous avez ajoutées à la table Mroute.

Supprimez une entrée de multidiffusion statique de la table Mroute IPv4

Vous pouvez supprimer une entrée de multidiffusion statique dont vous n'avez plus besoin de la table de routage IPv4.

Pour supprimer une entrée de multidiffusion statique de la table Mroute IPv4 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **roulage > Multicast > Configuration Mroute Static-Multicast**.
La page Configuration Mroute Static-Multicast s'affiche.
6. Cochez la case correspondant à l'entrée de multidiffusion.
7. Cliquez sur le bouton **Supprimer**.
Les paramètres sont enregistrés. L'entrée multicast est supprimée.
8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez les paramètres de multidiffusion globaux pour le commutateur

Vous pouvez configurer les paramètres de multidiffusion globaux du commutateur, par opposition aux paramètres de multidiffusion d'une interface.

Pour configurer les paramètres de multidiffusion globaux pour le commutateur :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > Multicast > Configuration globale**.

La page Configuration globale s'affiche.

6. Sélectionnez le bouton radio **Activer** ou **désactiver** le mode Admin pour activer ou désactiver l'état administratif du transfert multidiffusion sur le commutateur.

La valeur par défaut est désactiver.

7. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 130 : Informations de configuration globale multicast

Champ	Description
État du protocole	État opérationnel du transfert multidiffusion.
Nombre maximum d'entrées de la table	Nombre maximal d'entrées dans la table Mroute.
Protocole	Protocole de routage multicast actif sur le commutateur, si un protocole est actif.
Nombre d'entrées de table	Nombre d'entrées de route multicast présentes dans la table Mroute.

Configurer une interface multicast

Vous pouvez configurer une ou plusieurs interfaces multicast.

Pour configurer une interface multicast :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **roulage > Multicast > Configuration de l'interface**.

La page Configuration de l'interface s'affiche.

6. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :

- **1 ou ID d'unité pour un commutateur empilé :**

- 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.

- **ID d'unité pour un commutateur empilé :** Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.

- **VLAN** Seuls les VLAN sont affichés.

- **Tous:** Les interfaces physiques et les VLAN sont affichés, ou pour une pile de commutateurs, les interfaces physiques et les VLAN de tous les commutateurs sont affichés.

7. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :
 - Pour afficher ou effacer les statistiques d'une seule interface, cochez la case associée à l'interface ou saisissez le numéro de l'interface dans le champ **aller à l'interface** et cliquez sur le bouton **aller**.
 - Pour configurer plusieurs interfaces avec les mêmes paramètres, cochez la case associée à chaque interface.
 - Pour configurer toutes les interfaces avec les mêmes paramètres, cochez la case dans la ligne d'en-tête.
8. Dans le champ **TTL Threshold**, spécifiez le seuil en dessous duquel un paquet de données multidiffusion n'est pas transféré depuis l'interface.

Saisissez une valeur comprise entre 0 et 255. Le numéro par défaut est 1. Pour qu'un paquet soit transféré, sa valeur de durée de vie de multidiffusion (TTL) doit être supérieure à la valeur que vous avez définie. Si vous entrez 0, tous les paquets multicast sur l'interface sont transférés.
9. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.
10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Protocole DVMRP (Distance Vector Multicast Routing)

Le protocole DVMRP (distance Vector Multicast Routing Protocol) est utilisé pour la multidiffusion sur les réseaux IP sans protocoles de routage pour prendre en charge la multidiffusion. Le DVMRP est basé sur le protocole RIP mais plus complexe que le protocole RIP.

Le DVMRP fonctionne comme suit :

1. Le premier message (tel qu'un message IGMP) pour toute paire source-groupe est transmis à l'ensemble du réseau multidiffusion, par rapport au temps de vie (TTL) du paquet.
2. TTL restreint la zone à inonder par le message.
3. Tous les routeurs feuilles qui n'incluent pas de membres sur des sous-réseaux directement connectés renvoient des messages PRune au routeur en amont.

4. La branche qui transmet un message d'élaguage est supprimée de l'arbre de distribution.
5. L'arbre de diffusion, qui couvre tous les membres du groupe de multidiffusion, est construit.

De cette façon, DVRMP peut maintenir une base de données d'état de liens qui conserve la trace des chemins de retour à la source des paquets de multidiffusion.

Activez DVMRP sur le commutateur et affichez les informations d'itinéraire

Vous pouvez activer DVMRP sur le commutateur et afficher les informations d'itinéraire.

Pour activer DVMRP sur le commutateur et afficher les informations d'itinéraire globales :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > Multicast > DVMRP > Configuration globale** .

La page Configuration globale DVMRP s'affiche.

6. Sélectionnez un bouton radio mode Admin :
 - Activer. DVMRP est activé pour le commutateur.
 - Désactiver : DVMRP est désactivé pour le commutateur. Il s'agit de l'option par défaut.
7. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Champ	Description
Version	La version de protocole du DVMRP, qui est toujours 3.
Nombre total de routes	Nombre de routes dans la table de routage DVMRP.
Routes accessibles	Nombre de routes accessibles dans la table de routage DVMRP. Une route accessible a une métrique qui permet au commutateur d'atteindre le point final.

Configurer une interface DVMRP

Vous pouvez configurer une ou plusieurs interfaces DVMRP, qui sont des interfaces à partir desquelles le commutateur envoie des messages DVMRP qui permettent à l'arbre de distribution multicast de calculer le coût de route pour atteindre le commutateur.

Pour configurer une interface DVMRP :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > Multicast > DVMRP > Configuration de l'interface**.

La page Configuration de l'interface DVMRP s'affiche.

6. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :

- **1 ou ID d'unité pour un commutateur empilé :**
 - 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
 - **ID d'unité pour un commutateur empilé :** Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
- **VLAN** Seuls les VLAN sont affichés.
- **Tous:** Les interfaces physiques et les VLAN sont affichés, ou pour une pile de commutateurs, les interfaces physiques et les VLAN de tous les commutateurs sont affichés.

7. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :

- Pour configurer une interface ou un VLAN unique, cochez la case associée à l'interface ou au VLAN, ou tapez le numéro de l'interface ou du VLAN dans le champ **aller à l'interface** et cliquez sur le bouton **aller**.
- Pour configurer plusieurs interfaces ou VLAN avec les mêmes paramètres, cochez la case associée à chaque interface ou VLAN.

8. Dans le menu **interface mode**, sélectionnez si DVMRP est activé sur l'interface :

- Activer. DVMRP est activé pour l'interface.
- Désactiver : DVMRP est désactivé pour l'interface. Il s'agit de l'option par défaut.

9. Dans le champ **métrique de l'interface**, saisissez la métrique DVMRP de l'interface.

L'interface envoie la métrique dans des messages DVMRP qui indiquent le coût de route pour atteindre le commutateur. La plage est de 1 à 31. Le numéro par défaut est 1.

10. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

11. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Champ	Description
État du protocole	État opérationnel du protocole DVMRP sur l'interface : Opérationnel ou non opérationnel.
Adresse locale	Adresse IP utilisée comme adresse source dans les paquets envoyés depuis l'interface.
ID de génération	ID de génération DVMRP utilisé par le commutateur pour l'interface. Cet ID est réinitialisé chaque fois que l'interface est démarrée et est envoyé dans des messages PRune. Une modification de l'ID de génération informe les routeurs voisins qu'ils doivent supprimer toute information antérieure sur le commutateur.
Paquets incorrects reçus	Nombre de paquets Hello reçus sur l'interface.
Mauvais itinéraires reçus	Nombre de routes non valides reçues sur l'interface.
Itinéraires envoyés	Nombre de routes envoyées sur l'interface.

Afficher les voisins DVMRP

Si DVMRP est activé, vous pouvez afficher les voisins DVMRP.

Pour afficher les voisins DVMRP :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > Multicast > DVMRP > voisin DVMRP**.

La page de voisinage DVMRP s'affiche.

6. Pour rechercher un voisin, procédez comme suit :

- Dans le menu **Rechercher**, sélectionnez **interface** ou **IP voisin**.
- Dans le champ **Rechercher**, entrez un numéro d'interface au format unité/emplacement/port (par exemple, 1/0/14) ou une adresse IP, en fonction de votre sélection dans le menu.
- Cliquez sur le bouton **Go** (Accéder).

7. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

Les tableaux suivants décrivent les champs en lecture seule de la page.

Champ	Description
Interface	Interface pour laquelle les données sont affichées.
IP voisin	Adresse IP du voisin détectée par l'interface.
Etat	État du routeur voisin détecté par l'interface : actif ou inactif.
Durée de fonctionnement	Temps de disponibilité DVMRP pour le voisin tel que détecté par l'interface. Il s'agit de la période depuis que l'entrée voisine a été détectée par l'interface.
Heure d'expiration	Heure d'expiration DVMRP pour le voisin telle qu'elle est détectée par l'interface. Il s'agit de la période qui reste avant que l'entrée voisine ne vieillisse, et n'est pas applicable si l'état du routeur voisin est arrêté.
ID de génération	ID de génération DVMRP pour le voisin détecté par l'interface.
Version principale	Version majeure DVMRP pour le voisin détectée par l'interface. Par exemple, si le voisin exécute la version 3 de DVMRP, la version majeure est définie sur 0x03 et la version mineure sur 0xFF.
Version mineure	Version mineure DVMRP pour le voisin détectée par l'interface.

(A continué)

Champ	Description
Capacités	Capacités DVMRP du voisin détectées par l'interface.
Itinéraires reçus	Le nombre de routes reçues pour le voisin tel qu'il est détecté par l'interface.
Paquets incorrects reçus	Nombre de paquets non valides reçus pour le voisin, tel qu'il a été détecté par l'interface.
Mauvais itinéraires reçus	Nombre de routes non valides reçues pour le voisin, tel qu'il a été détecté par l'interface.

Afficher les sauts suivants du DVMRP

Si DVMRP est activé, vous pouvez afficher DVMRP les sauts suivants.

Pour afficher les sauts suivants du DVMRP :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

- Sélectionnez **routage > Multicast > DVMRP > saut suivant DVMRP**.

La page saut suivant DVMRP s'affiche.

❗ **Remarque:** Si vous choisissez d'afficher toutes les pages au lieu d'un nombre limité, l'affichage des informations peut prendre un certain temps.

- Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

Les tableaux suivants décrivent les champs en lecture seule de la page.

Champ	Description
Adresse IP source	Adresse IP utilisée avec le masque source pour identifier le réseau source
Masque source	Masque réseau utilisé avec l'adresse IP source
Interface de saut suivant	Interface du saut suivant qui se connecte à l'interface du commutateur
Type	Le type de saut suivant : Leaf signifie qu'aucun voisin dépendant en aval n'existe sur l'interface sortante. Sinon, le type est Branch. • Feuille: Aucun voisin dépendant en aval n'existe sur l'interface du tronçon suivant • Succursale: Des voisins dépendants en aval existent sur l'interface du tronçon suivant

Afficher le tableau DVMRP de l'élaguage

Si DVMRP est activé, vous pouvez afficher la table d'élaguage DVMRP, qui affiche les adresses IP du groupe de multidiffusion qui ont été supprimées de l'arborescence de diffusion de multidiffusion car elles ne desservent plus aucun membre de multidiffusion.

Pour afficher le tableau d'élaguage DVMRP :

- Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

- Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

- Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > Multicast > DVMRP > DVMRP Prune**.

La page DVMRP Prune s'affiche.

6. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

Les tableaux suivants décrivent les champs en lecture seule de la page.

Champ	Description
IP du groupe	Adresse IP du groupe qui a été élaguée.
Adresse IP source	Adresse IP utilisée avec le masque source pour identifier le réseau source.
Masque source	Masque réseau utilisé avec l'adresse IP source.
Heure d'expiration	Période restante avant l'expiration du pruneau au niveau du voisin en amont. Si aucun message d'élaguage n'est reçu des voisins en aval, cette période est définie sur la valeur de la durée de vie d'élaguage par défaut ; sinon, elle est définie sur la plus petite valeur reçue ou sur le temporisateur par défaut, selon la valeur la plus petite.

Afficher les itinéraires DVMRP

Si DVMRP est activé, vous pouvez afficher DVMRP les routes annoncées.

Pour afficher les itinéraires DVMRP :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > Multicast > DVMRP > route DVMRP** .

La page itinéraire DVMRP s'affiche.

6. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

Les tableaux suivants décrivent les champs en lecture seule de la page.

Table 131 : Informations de route DVMRP

Champ	Description
Adresse IP source	Adresse IP utilisée avec le masque source pour identifier le réseau source.
Masque source	Masque réseau utilisé avec l'adresse IP source.
Voisin en amont	Adresse du voisin amont (par exemple, un voisin de redirection de chemin inverse [RPF]) à partir duquel les datagrammes IP sont reçus.
Interface	Interface de commutation sur laquelle les datagrammes IP des voisins en amont sont reçus. Une valeur de 0 signifie que la route est un agrégat pour lequel aucune interface de saut suivant n'existe.
Métrique	Distance en sauts jusqu'au sous-réseau source.
Heure d'expiration	Période restante avant l'expiration de l'entrée de route.
Durée de fonctionnement	Période écoulée depuis que l'itinéraire a été détecté par le commutateur.

IGMP pour le routage multicast IPv4

Vous pouvez configurer les paramètres IGMP (Internet Group Management Protocol) et afficher les statistiques IGMP.

igmp snooping permet au commutateur de transférer intelligemment le trafic multicast. En fonction des messages de demandes et rapports IGMP, le switch transfère le trafic uniquement sur les ports qui ont demandé le trafic multicast.

igmp snooping aide à optimiser les performances de multidiffusion et est particulièrement utile pour les applications de multidiffusion IP gourmandes en bande passante, telles que les applications de streaming multimédia en ligne.

Activer ou désactiver IGMP pour le commutateur

Vous pouvez activer ou désactiver globalement IGMP pour le commutateur.

Pour configurer les paramètres IGMP globaux du commutateur :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **routage > Multicast > IGMP > Configuration globale** .
La page Configuration globale s'affiche.
6. Sélectionnez le bouton radio **Activer** ou **désactiver** le mode Admin pour activer ou désactiver IGMP sur le commutateur.
La valeur par défaut est désactiver.
7. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez une interface de routage IGMP

Vous pouvez configurer une ou plusieurs interfaces de routage IGMP.

Pour configurer une interface de routage IGMP :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > Multicast > IGMP > Configuration de l'interface de routage**.

La page Configuration de l'interface de routage s'affiche.

6. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :

- **1 ou ID d'unité pour un commutateur empilé :**

- 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
- **ID d'unité pour un commutateur empilé :** Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.

- VLAN Seuls les VLAN sont affichés.

- **Tous:** Les interfaces physiques et les VLAN sont affichés, ou pour une pile de commutateurs, les interfaces physiques et les VLAN de tous les commutateurs sont affichés.

7. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :

- Pour afficher ou effacer les statistiques d'une seule interface, cochez la case associée à l'interface ou saisissez le numéro de l'interface dans le champ **aller à l'interface** et cliquez sur le bouton **aller**.
- Pour configurer plusieurs interfaces avec les mêmes paramètres, cochez la case associée à chaque interface.
- Pour configurer toutes les interfaces avec les mêmes paramètres, cochez la case dans la ligne d'en-tête.

8. Dans le menu **mode Admin**, sélectionnez **Activer** ou **désactiver** pour activer ou désactiver IGMP pour l'interface.

La valeur par défaut est désactiver.

9. Dans le champ **version**, spécifiez la version d'IGMP pour l'interface.

La version peut être 1, 2 ou 3. Le numéro par défaut est 3. Ce champ est configurable uniquement lorsque le mode interface IGMP est activé.

10. Dans le champ **robustesse**, saisissez la valeur de robustesse de l'interface.

La valeur de robustesse permet un réglage pour compenser la perte de paquets attendue sur un sous-réseau. IGMP est robuste aux pertes de paquets (valeur de robustesse - 1). Si vous pensez que le sous-réseau sera avec perte, entrez un nombre plus élevé. La valeur est comprise entre 1 et 255. Le numéro par défaut est 2.

11. Dans le champ **intervalle de requête**, entrez la fréquence en secondes à laquelle les paquets de requête d'appartenance à l'hôte IGMP sont transmis sur l'interface.
La valeur est comprise entre 1 et 3600. Le numéro par défaut est 125.
12. Dans le champ **Query Max Response Time**, entrez le temps de réponse maximal à la requête, en dixièmes de seconde, pour qu'un rapport d'appartenance soit reçu avant l'expiration de la requête IGMPv2 sur l'interface.
La valeur est comprise entre 0 et 255. Le numéro par défaut est 100.
13. Dans le champ **intervalle de requête de démarrage**, entrez le nombre de secondes entre la transmission des requêtes de démarrage sur l'interface.
La valeur est comprise entre 1 et 300. Le numéro par défaut est 31.
14. Dans le champ **nombre de requêtes de démarrage**, entrez le nombre de requêtes à envoyer au démarrage, le temps entre les requêtes étant déterminé par l'intervalle de requête de démarrage.
La valeur est comprise entre 1 et 20. Le numéro par défaut est 2.
15. Dans le champ **intervalle de requête du dernier membre**, entrez le dernier intervalle de requête du membre en dixièmes de seconde.
Cette valeur est le temps de réponse maximal à insérer dans les requêtes spécifiques au groupe envoyées en réponse aux messages Leave Group, et est également la période entre les messages de requête spécifiques au groupe. La valeur est comprise entre 0 et 255. Le numéro par défaut est 10. Cette valeur n'est pas utilisée pour IGMP version 1.
16. Dans le champ **nombre de requêtes du dernier membre**, entrez le nombre de requêtes à envoyer lors de la réception d'un rapport de groupe de congés.
La valeur est comprise entre 1 et 20. Le numéro par défaut est 2.
17. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
18. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Affiche les statistiques des interfaces de routage IGMP

Vous pouvez afficher les statistiques des interfaces de routage IGMP.

Pour afficher les statistiques des interfaces de routage IGMP :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > Multicast > IGMP > statistiques de l'interface de routage**.

La page Routing interface Statistics s'affiche.

6. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :

- **1 ou ID d'unité pour un commutateur empilé :**
 - 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
 - **ID d'unité pour un commutateur empilé :** Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
- **VLAN** Seuls les VLAN sont affichés.
- **Tous:** Les interfaces physiques et les VLAN sont affichés, ou pour une pile de commutateurs, les interfaces physiques et les VLAN de tous les commutateurs sont affichés.

7. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

Le tableau suivant décrit les champs en lecture seule de la page.

Table 132 : Informations statistiques de l'interface de routage IGMP

Champ	Description
Interface	Interface sur laquelle IGMP est activé.
Adresse IP	Adresse IP de l'interface.
Masque de sous-réseau	Masque de sous-réseau pour l'adresse IP de l'interface.
État du protocole	État opérationnel de l'IGMP sur l'interface (opérationnel ou non opérationnel).
Querier IP	Adresse du questeur IGMP sur le sous-réseau IP auquel l'interface est rattachée.
Statut Querier	Indique si l'interface est en mode interrogateur ou non interrogateur.
Querier Up Time	Période en secondes depuis la dernière modification du questionneur de l'interface IGMP.
Délai d'expiration du Querier	La période en secondes restante avant l'expiration de l'autre temporisateur de présence de l'interrogateur. Si le commutateur est l'interrogateur, cela vaut zéro.
Requêtes de version erronées reçues	Nombre de requêtes reçues sur l'interface avec une version IGMP qui ne correspond pas à la version IGMP configurée pour l'interface, pendant la durée de vie de l'entrée. IGMP exige que tous les routeurs ou interfaces de routage sur un LAN soient configurés pour exécuter la même version d'IGMP. Par conséquent, une erreur de configuration est indiquée si des requêtes sont reçues avec un numéro de version incorrect.
Nombre de joints reçus	Nombre de fois qu'une appartenance à un groupe a été ajoutée sur l'interface, c'est-à-dire le nombre de fois qu'une entrée pour l'interface a été ajoutée à la table de cache. Cela donne une indication de la quantité d'activité IGMP sur l'interface.
Nombre de groupes	Nombre actuel d'entrées pour l'interface dans la table cache.

Affichez les groupes IGMP et effectuez une recherche dans la base de données des groupes IGMP

Vous pouvez afficher les informations du groupe IGMP et rechercher dans la base de données des groupes IGMP par interface ou par groupe.

Pour afficher les groupes IGMP et effectuer une recherche dans la base de données des groupes IGMP :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > Multicast > IGMP > IGMP Groups**.

La page groupes IGMP s'affiche.

6. Pour rechercher des entrées de groupe IGMP par interface ou par groupe, sélectionnez l'une des options suivantes dans le menu **Rechercher** :

- Interface Sélectionnez **interface** dans le menu, spécifiez l'interface au format unité/port (par exemple 0/8), puis cliquez sur le bouton **aller**.

Si l'entrée existe, l'entrée est affichée en tant que première entrée, suivie des entrées restantes.

- Groupe Sélectionnez **Groupe** dans le menu, spécifiez l'adresse IPv4 du groupe de multidiffusion, puis cliquez sur le bouton **aller**.

Si l'entrée existe, l'entrée avec l'adresse IPv4 de groupe correspondante est affichée comme première entrée, suivie des entrées restantes. Une correspondance exacte est requise.

7. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

Le tableau suivant décrit les champs en lecture seule de la page.

Table 133 : Informations sur le groupe IGMP

Champ	Description
Interface	Interface sur laquelle IGMP est activé.
IP du groupe de multidiffusion	Adresse du groupe de multidiffusion IP.
Dernier reporter	Adresse IP de la source du dernier rapport d'appartenance reçu pour l'adresse du groupe de multidiffusion IP sur l'interface.
Durée de fonctionnement	Période écoulée depuis la création de cette entrée.
Heure d'expiration	Période restante avant expiration de cette entrée.
Temporisateur hôte version 1	Période restante jusqu'à ce que le commutateur détermine qu'aucun membre IGMP version 1 ne se trouve sur le sous-réseau IP connecté à l'interface. Lorsqu'un rapport d'appartenance IGMPv1 est reçu, ce temporisateur est réinitialisé sur le temporisateur d'appartenance au groupe. À moins que ce temporisateur n'atteigne zéro, le commutateur ignore tout message IGMPv2 Leave pour ce groupe que informatique reçoit sur l'interface. Ce champ s'affiche uniquement si l'interface est configurée pour IGMP version 1.
Temporisateur hôte version 2	Temps restant avant que le commutateur ne détermine qu'aucun membre IGMP version 2 ne se trouve sur le sous-réseau IP connecté à l'interface. Lorsqu'un rapport d'appartenance IGMPv2 est reçu, ce temporisateur est réinitialisé sur le temporisateur d'appartenance au groupe. À moins que ce temporisateur n'atteigne zéro, le commutateur ignore les messages IGMPv1 et IGMPv3 Leave pour ce groupe que informatique reçoit sur l'interface sélectionnée. Ce champ s'affiche uniquement si l'interface est configurée pour IGMP version 2.
Compatibilité	Mode de compatibilité de groupe (v1, v2 ou v3) pour le groupe sur l'interface.
Mode de filtrage	Le mode de filtre source (inclure, exclure ou NA) pour le groupe sur l'interface. Si le mode est NA, le champ est vide.

Affichez les informations d'adhésion IGMP et effectuez une recherche dans la base de données d'adhésion IGMP

Vous pouvez afficher les informations d'appartenance IGMP et rechercher dans la base de données d'appartenance IGMP par interface ou par groupe.

Pour afficher les informations relatives à l'adhésion à IGMP et effectuer une recherche dans la base de données d'adhésion à IGMP :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > Multicast > IGMP > IGMP Membership**.

La page adhésion IGMP s'affiche.

6. Pour rechercher une appartenance IGMP par interface ou groupe, sélectionnez l'une des options suivantes dans le menu **Rechercher** :

- Interface Sélectionnez **interface** dans le menu, spécifiez l'interface au format unité/port (par exemple 0/8), puis cliquez sur le bouton **aller**.

Si l'entrée existe, l'entrée est affichée en tant que première entrée, suivie des entrées restantes.

- Groupe Sélectionnez **Groupe** dans le menu, spécifiez l'adresse IP du groupe de multidiffusion, puis cliquez sur le bouton **aller**.

Si l'entrée existe, l'entrée avec l'adresse IP du groupe correspondante est affichée en première entrée, suivie des entrées restantes. Une correspondance exacte est requise.

7. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

Le tableau suivant décrit les champs en lecture seule de la page.

Table 134 : Informations d'adhésion IGMP

Champ	Description
Interface	Interface sur laquelle les paquets multicast sont transmis.
IP du groupe	Adresse du groupe de multidiffusion IP.
Mode de compatibilité	Mode de compatibilité de groupe (v1, v2 ou v3) pour le groupe sur l'interface.
Mode filtre source	Le mode de filtre source (inclure, exclure ou NA) pour le groupe sur l'interface. Si le mode est NA, le champ est vide.
Hôtes sources	Adresses IP source membres de l'adresse de multidiffusion.
Heure d'expiration	Délai d'expiration qui s'applique à chaque adresse IP source membre du groupe de multidiffusion. Il s'agit de la période au bout de laquelle l'entrée de la source expire.

Configurez une interface proxy IGMP

Vous pouvez configurer une interface proxy IGMP. Les exigences suivantes s'appliquent :

- Le routage, l'IGMP et la multidiffusion doivent être globalement activés sur le commutateur.
- Vous devez configurer au moins une interface de routage.
- L'interface proxy IGMP ne peut pas être la même qu'une interface de routage IGMP.

Pour configurer une interface proxy IGMP :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **routage > Multicast > IGMP > Configuration de l'interface proxy**.
La page Configuration de l'interface proxy s'affiche.
6. Dans le menu **interface**, sélectionnez l'interface qui doit fonctionner comme interface proxy IGMP.
7. Dans le menu **mode Admin**, sélectionnez **Activer** ou **désactiver** pour activer ou désactiver la fonction proxy IGMP sur l'interface.
La valeur par défaut est désactiver.
8. Dans le champ **intervalle de rapport non sollicité**, spécifiez la période en secondes entre les répétitions du rapport initial d'un hôte sur l'appartenance à un groupe.
La plage est de 1 à 260. Le numéro par défaut est 1.
9. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 135 : Informations de configuration de l'interface proxy IGMP

Champ	Description
Adresse IP	Adresse IP de l'interface proxy IGMP.
Masque de sous-réseau	Masque de sous-réseau pour l'adresse IP de l'interface proxy IGMP.
Mode de fonctionnement	État opérationnel de l'interface proxy IGMP (désactiver ou Activer).
Adresse du Querier sur l'interface proxy	Adresse de l'interrogeur sur l'interface proxy.

Table 135 : Informations de configuration de l'interface proxy IGMP (A continué)

Champ	Description
Nombre de groupes	Nombre d'entrées de groupe de multidiffusion pour l'interface proxy IGMP dans la table cache.
Version	Version d'IGMP configurée sur l'interface de routage IGMP que vous avez transformée en interface proxy IGMP. Pour plus d'informations, consultez la section Configurez une interface de routage IGMP à la page 697.
Expiration du délai du Querier version 1	Délai d'expiration du interrogateur IGMPv1 en secondes. Si un hôte reçoit une requête IGMPv1, il définit temporairement son temporisateur de présence de requête IGMPv1 sur l'intervalle de requête IGMPv1. Une fois que l'hôte a lu la requête IGMPv1, le délai d'expiration de l'interrogateur IGMPv1 indique la période après laquelle l'hôte repasse à IGMPv3.
Version 2 Querier Timeout	Délai d'expiration du interrogateur IGMPv2 en secondes. Si un hôte reçoit une requête IGMPv2, il définit temporairement son temporisateur de présence de l'interrogateur IGMPv2 sur l'intervalle de l'interrogateur IGMPv2. Une fois que l'hôte a lu la requête IGMPv2, le délai d'expiration du interrogateur IGMPv2 indique la période après laquelle l'hôte repasse à IGMPv3.
Fréquence de démarrage du proxy	Le nombre de fois où le proxy a été démarré.

Affiche les statistiques de l'interface proxy IGMP

Vous pouvez afficher les statistiques de l'interface proxy IGMP.

Pour afficher les statistiques de l'interface proxy IGMP :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > Multicast > IGMP > Proxy interface Statistics**.

La page statistiques de l'interface proxy s'affiche.

6. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

Le tableau suivant décrit les champs en lecture seule de la page.

Table 136 : Informations statistiques sur l'interface proxy IGMP

Champ	Description
Interface proxy	Interface sur laquelle les paquets IGMP sont reçus.
Version	Version des paquets IGMP reçus.
Requêtes reçues	Nombre de requêtes IGMP reçues.
Rapport reçu	Le nombre de rapports IGMP reçus.
Rapports envoyés	Nombre de rapports IGMP envoyés.
Congés reçus	Nombre de messages IGMP Leave reçus.
Feuilles envoyées	Nombre de messages IGMP Leave envoyés.

Affichez l'appartenance au proxy IGMP et recherchez dans la base de données d'appartenance au proxy IGMP

Vous pouvez afficher les informations d'appartenance au proxy IGMP et rechercher la base de données d'appartenance au proxy IGMP par groupe.

Pour afficher les informations d'appartenance au proxy IGMP et effectuer une recherche dans la base de données d'appartenance au proxy IGMP :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > Multicast > IGMP > Proxy Membership**.

La page adhésion au proxy s'affiche.

6. Pour rechercher l'appartenance à un proxy IGMP par groupe, spécifiez l'adresse IPv4 du groupe de multidiffusion, puis cliquez sur le bouton **aller**.

Si l'entrée existe, l'entrée avec l'adresse IPv4 de groupe correspondante est affichée comme première entrée, suivie des entrées restantes. Une correspondance exacte est requise.

7. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

Le tableau suivant décrit les champs en lecture seule de la page.

Table 137 : Informations d'appartenance au proxy IGMP

Champ	Description
Interface proxy	Interface sur laquelle le proxy IGMP est activé.
IP du groupe	Adresse IPv4 du groupe de multidiffusion.
Hôtes sources	Adresses sources membres du groupe multicast.
Dernier reporter	Adresse IPv4 source qui a envoyé le dernier rapport d'appartenance pour le groupe de multidiffusion sur l'interface proxy IGMP.
Durée de fonctionnement	Temps écoulé depuis la création de l'entrée.
Heure d'expiration	Intervalle d'expiration de chaque adresse source membre du groupe de multidiffusion. Il s'agit de la période au bout de laquelle l'entrée de la source expire.
Etat	État de l'entrée hôte : • Etat non membre : L'hôte n'appartient pas au groupe sur l'interface. • Retarder l'État membre : L'hôte appartient au groupe sur l'interface et son temporisateur de rapport est actif. (La minuterie de rapport est utilisée pour envoyer des rapports.) • Etat membre inactif : L'hôte appartient au groupe sur l'interface mais son temporisateur de rapport est inactif.
Mode de filtrage	Le mode de filtre de groupe (inclure, exclure ou aucun) pour le groupe sur l'interface proxy IGMP.
Nombre de sources	Nombre d'hôtes source dans le groupe de multidiffusion.

PIM pour le routage multicast IPv4

Protocole PIM (Protocol-Independent Multicast) est un protocole de routage multicast standard qui fournit un routage multicast interdomaine évolutif sur Internet, indépendant de tout protocole de routage unicast particulier.

Vous pouvez configurer les différents paramètres PIM pour le routage multicast IPv4 et afficher les statistiques PIM.

Configurez les paramètres IPv4 PIM globaux sur le commutateur

En fonction des besoins de votre réseau IPv4, vous pouvez activer globalement le mode PIM Sparse (PIM-SM) ou le mode PIM dense (PIM-DM) sur le commutateur.

Pour configurer les paramètres IPv4 PIM globaux sur le commutateur :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routing > Multicast > PIM > Configuration globale**.

La page Configuration globale s'affiche.

6. Sélectionnez l'un des boutons radio mode Admin suivants :

- Désactiver : Le module PIM est désactivé sur le commutateur. Il s'agit de l'option par défaut.
- **PIM-SM** : Le mode épars PIM est activé sur le commutateur.
- PIM-DM Le mode dense PIM est activé sur le commutateur.

7. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Ajouter des groupes PIM-SSM IPv4

Alors que PIM utilise un routeur de point de rendez-vous (RP) spécialement configuré qui sert de jonction de réunion pour les expéditeurs et les auditeurs de multidiffusion, PIM Single-source Multicast (PIM-SSM) n'utilise pas de point de rendez-vous (RP). PIM-SSM prend uniquement en charge les arborescences de livraison de route source. informatique est utilisé entre les routeurs (y compris les interfaces de routeur de commutateur) afin qu'ils puissent suivre les paquets de multidiffusion à transmettre les uns aux autres et à leurs réseaux locaux directement connectés. Vous pouvez implémenter PIM-SSM avec un sous-ensemble strict des mécanismes du protocole PIM. La multidiffusion IPv4 régulière et SSM peuvent coexister sur un même routeur, et les deux peuvent être implémentés à l'aide du protocole PIM. Une plage d'adresses multicast, 232.0,0.0/8 pour IPv4, est réservée à SSM.

Pour ajouter un groupe PIM-SSM IPv4 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routing > Multicast > PIM > Configuration SSM**.

L'écran SSM Configuration (Configuration IP) s'affiche.

6. Dans le champ **adresse du groupe SSM**, spécifiez l'adresse IPv4 du groupe de multidiffusion spécifique à la source.
7. Dans le champ **masque de groupe SSM**, spécifiez le masque de l'adresse IPv4 du groupe de multidiffusion spécifique à la source.
8. Cliquez sur le bouton **Add** (Ajouter).
Les paramètres sont enregistrés. Le groupe est ajouté.
9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimer un groupe PIM-SSM IPv4

Vous pouvez supprimer un groupe PIM-SSM IPv4 dont vous n'avez plus besoin.

Pour supprimer un groupe PIM-SSM IPv4 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.
4. Cliquez sur le bouton **Login** (Connexion).
La page System Information (Informations système) s'affiche.
5. Sélectionnez **roulage > Multicast > Configuration Mroute Static-Multicast**.

La page Configuration Mroute Static-Multicast s'affiche.

6. Cochez la case correspondant au groupe PIM-SSM.

7. Cliquez sur le bouton **Supprimer**.

Les paramètres sont enregistrés. Le groupe PIM-SSM est supprimé.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurer une interface PIM IPv4

Vous pouvez configurer une interface IPv4 pour PIM.

Pour configurer une interface PIM IPv4 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routing > Multicast > PIM > Configuration de l'interface** .

La page Configuration de l'interface s'affiche.

6. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :
 - **1 ou ID d'unité pour un commutateur empilé :**
 - 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
 - **ID d'unité pour un commutateur empilé :** Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
 - **VLAN** Seuls les VLAN sont affichés.
 - **Tous:** Les interfaces physiques et les VLAN sont affichés, ou pour une pile de commutateurs, les interfaces physiques et les VLAN de tous les commutateurs sont affichés.
7. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :
 - Pour afficher ou effacer les statistiques d'une seule interface, cochez la case associée à l'interface ou saisissez le numéro de l'interface dans le champ **aller à l'interface** et cliquez sur le bouton **aller**.
 - Pour configurer plusieurs interfaces avec les mêmes paramètres, cochez la case associée à chaque interface.
 - Pour configurer toutes les interfaces avec les mêmes paramètres, cochez la case dans la ligne d'en-tête.
8. Dans le menu **mode Admin**, sélectionnez **Activer** ou **désactiver** pour activer ou désactiver PIM pour l'interface.

La valeur par défaut est désactiver.
9. Dans le champ **intervalle Hello**, spécifiez la période en secondes entre la transmission des messages Hello PIM sur l'interface.

La plage est de 0 à 18000. Le numéro par défaut est 30.
10. Dans le champ **intervalle de jointure/élagage**, spécifiez la période en secondes à laquelle les messages PIM Join/élagage sont transmis sur l'interface.

La plage est de 0 à 18000. Le numéro par défaut est 60.
11. Dans le menu **BSR Border**, sélectionnez **Enable (Activer)** ou **Disable (désactiver)** pour activer ou désactiver la bordure du routeur d'amorçage (BSR) sur l'interface.

La valeur par défaut est désactiver.
12. Dans le champ **priorité DR**, spécifiez la priorité du routeur désigné (DR) pour l'interface.

La plage est de 0 à 2147483647. Le numéro par défaut est 1.
13. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

14. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 138 : Informations de configuration de l'interface PIM IPv4

Champ	Description
État du protocole	État du PIM sur l'interface (opérationnel ou non opérationnel).
Adresse IP	Adresse IPv4 de l'interface PIM.
Routeur désigné	Adresse IPv4 du routeur désigné sur l'interface PIM.
Nombre de voisins	Nombre de voisins PIM sur l'interface PIM.

Afficher les voisins PIM IPv4 et rechercher la base de données des voisins PIM

Vous pouvez afficher les informations de voisinage PIM IPv4 et rechercher dans la base de données de voisins PIM par interface ou par adresse IP de voisin.

Pour afficher les voisins PIM IPv4 et effectuer une recherche dans la base de données des voisins PIM :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
 Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
 La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
 La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > Multicast > PIM > voisin PIM**.

La page de voisinage PIM s'affiche.

6. Pour rechercher des entrées de groupe IGMP par interface ou par groupe, sélectionnez l'une des options suivantes dans le menu **Rechercher** :

- Interface Sélectionnez **interface** dans le menu, spécifiez l'interface au format unité/port (par exemple 0/8), puis cliquez sur le bouton **aller**.
Si l'entrée existe, l'entrée est affichée en tant que première entrée, suivie des entrées restantes.
- IP voisin Sélectionnez **IP voisin** dans le menu, spécifiez l'adresse IPv4 du voisin, puis cliquez sur le bouton **aller**.
Si l'entrée existe, l'entrée avec l'adresse IPv4 voisine correspondante est affichée comme première entrée, suivie des entrées restantes. Une correspondance exacte est requise.

7. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

Le tableau suivant décrit les champs en lecture seule de la page.

Table 139 : Informations de voisinage PIM IPv4

Champ	Description
Interface	Interface sur laquelle le PIM voisin est connecté.
IP voisin	Adresse IPv4 du voisin PIM.
Temps de fonctionnement (hh:mm:ss)	Temps écoulé depuis que le périphérique PIM est devenu un voisin de l'interface.
Heure d'expiration (hh:mm:ss)	Le temps restant avant que le PIM voisin ne vieillisse.
Priorité DR	Priorité de routeur désigné (DR) du voisin PIM.

Ajoutez une configuration de point de rendez-vous candidat PIM IPv4

Vous pouvez ajouter une configuration de point de rendez-vous candidat PIM IPv4 sur une interface.

Pour ajouter une configuration RP candidate PIM IPv4 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **roulage > Multicast > PIM > Configuration RP candidate** .

La page Configuration du RP candidat s'affiche.

6. Dans le menu **interface**, sélectionnez l'interface.

7. Dans le champ **adresse du groupe**, spécifiez l'adresse IPv4 du groupe qui est transmise dans les annonces RP-candidates.

8. Dans le champ **masque de groupe**, saisissez le masque d'adresse de groupe transmis dans les annonces RP-candidates.

9. Dans le champ **intervalle d'annonce C-RP**, spécifiez la période en secondes pendant laquelle les annonces RP-candidates sont envoyées en tant que trafic de monodiffusion au routeur d'amorçage (BSR).

La plage est de 1 à 16383 secondes.

10. Cliquez sur le bouton **Add** (Ajouter).

Les paramètres sont enregistrés. Le RP candidat PIM est ajouté.

11. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimer une configuration de point de rendez-vous candidat PIM IPv4

Vous pouvez supprimer une configuration de point de rendez-vous candidat PIM IPv4 dont vous n'avez plus besoin.

Pour supprimer une configuration RP candidate PIM IPv4 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **roulage > Multicast > PIM > Configuration RP candidate**.

La page Configuration du RP candidat s'affiche.

6. Dans le menu **interface**, sélectionnez l'interface.
7. Cochez la case correspondant au RP candidat PIM.
8. Cliquez sur le bouton **Supprimer**.

Les paramètres sont enregistrés. L'entrée RP candidat PIM est supprimée.

Configurez une interface comme candidat routeur d'amorçage PIM IPv4

Vous pouvez configurer une interface en tant que candidat au routeur d'amorçage PIM (BSR) IPv4.

Pour configurer une interface en tant que candidat BSR PIM IPv4 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routing > Multicast > PIM > Configuration candidat BSR**.

La page Configuration du candidat BSR s'affiche.

6. Dans le menu **interface**, sélectionnez une interface.
7. Dans le champ **longueur du masque de hachage**, spécifiez la longueur du masque de hachage à annoncer dans les messages d'amorçage.

La longueur du masque de hachage est utilisée dans l'algorithme de hachage pour sélectionner le RP d'un groupe particulier. La plage est de 0 à 32. Le numéro par défaut est 30.

8. Dans le champ **priorité**, spécifiez la priorité du candidat BSR.

La plage est de 0 à 255. Le numéro par défaut est 0.

9. Dans le champ **intervalle d'annonce**, spécifiez la période en secondes entre les annonces.

La plage est de 1 à 16383. Le numéro par défaut est 60.

10. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

11. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

12. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

Le tableau suivant décrit les champs en lecture seule de la page.

Table 140 : Informations de configuration candidate BSR PIM IPv4

Champ	Description
Délai d'expiration BSR (hh:mm:ss)	Durée (en heures, minutes et secondes) après laquelle le BSR sélectionné appréhendé expire.
Adresse IP	Adresse IPv4 du BSR sélectionné.
Message d'amorçage suivant (hh:mm:ss)	Temps (en heures, minutes et secondes) après lequel le prochain message d'amorçage est dû à partir du BSR.
Annonce RP du candidat suivant (hh:mm:ss)	Durée (en heures, minutes et secondes) après laquelle la prochaine annonce RP de candidat est envoyée.

Supprimez une configuration candidate de routeur d'amorçage PIM IPv4

Vous pouvez supprimer une configuration candidate de routeur d'amorçage PIM (BSR) IPv4 d'une interface.

Pour supprimer une configuration candidate BSR PIM IPv4 d'une interface :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routing > Multicast > PIM > Configuration candidat BSR**.

La page Configuration du candidat BSR s'affiche.

6. Dans le menu **interface**, sélectionnez l'interface.

7. Cliquez sur le bouton **Supprimer**.

Les paramètres sont enregistrés. La configuration candidate PIM BSR est supprimée de l'interface.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez un point de rendez-vous PIM IPv4 statique pour un groupe

Vous pouvez ajouter un nouveau point de rendez-vous PIM IPv4 statique ou modifier un point de rendez-vous (RP) IPv4 existant pour un groupe.

Pour ajouter ou modifier un PIM RP IPv4 statique pour un groupe :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **roulage > Multicast > PIM > Configuration RP statique** .

La page Configuration RP statique s'affiche.

6. Si vous modifiez un RP statique existant, cochez la case correspondant au RP statique.
7. Dans le champ **adresse RP**, spécifiez l'adresse IPv4 du RP statique.
8. Dans le champ **adresse du groupe**, spécifiez l'adresse IPv4 du groupe auquel s'applique le RP statique.
9. Dans le champ **masque de groupe**, spécifiez le masque du groupe auquel s'applique le RP statique.

10. Dans le menu **Override**, sélectionnez **Enable** ou **Disable** pour activer ou désactiver la capacité de remplacement d'un RP statique sur un RP appris à partir d'un BSR.

Si vous sélectionnez **Activer** et qu'un conflit se produit, un RP statique remplace un RP appris à partir d'un BSR.

11. Effectuez l'une des opérations suivantes :

- Si vous ajoutez un nouveau RP statique, cliquez sur le bouton **Ajouter**.
Les paramètres sont enregistrés. Le RP statique est ajouté.
- Si vous modifiez un RP statique existant, cliquez sur le bouton **appliquer**.
Les paramètres sont enregistrés.

12. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimer une configuration de point de rendez-vous PIM IPv4 statique

Vous pouvez supprimer une configuration de point de rendez-vous (RP) PIM IPv4 statique dont vous n'avez plus besoin pour un groupe.

Pour supprimer une configuration PIM RP IPv4 statique pour un groupe :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > Multicast > PIM > Configuration RP statique**.

La page Configuration RP statique s'affiche.

6. Cochez la case du RP statique.

7. Cliquez sur le bouton **Supprimer**.

Les paramètres sont enregistrés. La configuration RP statique est supprimée pour le groupe.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Routes de multidiffusion statiques pour les adresses IPv4

Si un protocole de routage multicast tel que PIM-SM ou PIM-DM est activé et configuré, les routes multicast sont construites dynamiquement. Toutefois, vous pouvez également configurer une ou plusieurs routes de multidiffusion IPv4 statiques. Une route statique peut faciliter le traitement du trafic de multidiffusion lorsqu'un routeur de redirection de chemin inverse (RPF) voisin est situé entre le commutateur et la source de multidiffusion.

Configurer des routes de multidiffusion statiques pour les adresses IPv4

Vous pouvez ajouter une nouvelle route de multidiffusion IPv4 statique ou modifier une route existante.

Pour ajouter ou modifier une route de multidiffusion IPv4 statique :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **roulage > Multicast > Configuration des routes statiques** .

La page Configuration des routes statiques s'affiche.

6. Si vous modifiez une route de multidiffusion statique existante, cochez la case de la route.

Pour une route statique existante, vous pouvez uniquement modifier la métrique.

7. Dans le champ **source IP**, spécifiez l'adresse IPv4 de la source du paquet multicast.
8. Dans le champ **masque source**, spécifiez le masque de sous-réseau de la source du paquet multidiffusion.

9. Dans le champ **voisin RPF**, spécifiez l'adresse IPv4 du routeur RPF voisin situé entre le commutateur et la source de multidiffusion.
10. Dans le champ **métrique**, spécifiez le coût de l'état de la liaison du chemin de la source de multidiffusion au commutateur.
La plage est de 0 à 255.
11. Effectuez l'une des opérations suivantes :
 - Si vous ajoutez une nouvelle route de multidiffusion statique, cliquez sur le bouton **Ajouter**.
Les paramètres sont enregistrés. La route de multidiffusion statique est ajoutée.
 - Si vous modifiez une route de multidiffusion statique existante, cliquez sur le bouton **appliquer**.
Les paramètres sont enregistrés.
12. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimer une route de multidiffusion statique pour une adresse IPv4

Vous pouvez supprimer une route de multidiffusion IPV4 statique dont vous n'avez plus besoin.

Pour supprimer une route de multidiffusion IPv4 statique :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **roulage > Multicast > Configuration des routes statiques**.

La page Configuration des routes statiques s'affiche.

6. Cochez la case de la route statique.

7. Cliquez sur le bouton **Supprimer**.

Les paramètres sont enregistrés. La route statique est supprimée.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Limites d'administration multicast pour les adresses IPv4

Une limite administrative de multidiffusion (admin) peut arrêter le trafic de multidiffusion en entrée et en sortie pour une plage d'adresses de multidiffusion sur l'interface de routage. À l'aide des limites d'administration, vous pouvez définir les limites d'une région de multidiffusion, au-delà de laquelle le trafic de multidiffusion n'est pas censé traverser.

Configurer une interface en tant que limite d'administration multicast

Vous pouvez configurer une interface en tant que limite d'administration multicast.

Pour configurer une interface en tant que limite d'administration multicast :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **roulage > Multicast > Admin Boundary Configuration**.

La page Admin Boundary Configuration s'affiche.

6. Dans le menu **interface**, sélectionnez l'interface.

7. Dans le champ **IP du groupe**, spécifiez l'adresse du groupe de multidiffusion pour le début de la plage d'adresses à exclure.

L'adresse doit être comprise entre 239.0.0.0 et 239.255.255.255.

8. Dans le champ **masque de groupe**, entrez le masque de l'adresse du groupe de multidiffusion.

La combinaison du masque et de l'adresse IP du groupe définit la plage de la limite d'administration multicast.

9. Cliquez sur le bouton **Add** (Ajouter).

Les paramètres sont enregistrés. La limite d'administration multicast est ajoutée.

10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimer une configuration de limite d'administration multicast pour une interface

Vous pouvez supprimer une configuration de limite d'administration multicast dont vous n'avez plus besoin pour une interface.

Pour supprimer une configuration de limite d'administration multicast :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > Multicast > Admin Boundary Configuration**.

La page Admin Boundary Configuration s'affiche.

6. Cochez les cases correspondant au contenu.

7. Cliquez sur le bouton **Supprimer**.

Les paramètres sont enregistrés. La route statique est supprimée de l'interface.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Routage multicast IPv6 et table de routage multicast IPv6

La multidiffusion est particulièrement adaptée au trafic vidéo et audio nécessitant un contrôle des paquets de multidiffusion pour un fonctionnement optimal. Multicast pour IPv6 inclut la prise en charge de Multicast Listener Discovery (MLD). La communication de point à multipoint est appelée multidiffusion. L'hôte source (point) transmet un message à un groupe de zéro hôte ou plus (multipoint) identifiés par une adresse de destination IPv6 unique. Bien que la tâche puisse être accomplie en envoyant des messages unicast (point à point) à chacun des hôtes de destination, la multidiffusion est la méthode préférée pour ce type de transmission. Un message de multidiffusion est remis à tous les membres de son groupe d'hôtes de destination avec la même fiabilité que les messages IPv6 monodiffusion réguliers. Il n'est pas garanti que le message arrive intact à tous les membres du groupe de destination ou dans le même ordre par rapport aux autres messages.

Affichez la table de routage multicast IPv6

La table de routage multicast (Mroute) comprend des informations sur l'adresse IPv6 source, les adresses IPv6 de destination du groupe, les interfaces entrante et sortante, les sauts suivants vers lesquels le paquet IPv6 doit être transféré et les protocoles pris en charge.

Pour afficher la table Mroute IPv6 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **roulage > Multicast IPv6 > table Mroute** .

La page table Mroute s'affiche.

6. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

Le tableau suivant décrit les champs en lecture seule de la page.

Table 141 : Informations de table Mroute IPv6 multicast

Champ	Description
IP du groupe	Adresse IPv6 du groupe de destination.
Adresse IP source	Adresse IPv6 de la source de paquets multicast à combiner avec le groupe IPv6 pour identifier entièrement la route unique.
Interface entrante	Interface entrante sur laquelle arrivent les paquets multicast pour cette source/ce groupe.
Interfaces sortantes	Liste des interfaces sortantes sur lesquelles les paquets multicast pour cette source/ce groupe sont transmis.
Temps de fonctionnement (hh:mm:ss)	Temps en secondes depuis la création de l'entrée.
Heure d'expiration (hh:mm:ss)	Temps en secondes avant que cette entrée ne vieillisse et ne soit supprimée du tableau.
Voisin RPF	Adresse IPv6 du voisin de redirection de chemin inverse (RPF).

Table 141 : Informations de table Mroute IPv6 multicast (A continué)

Champ	Description
Protocole	Protocole de routage multicast qui a créé dynamiquement cette entrée. Les valeurs possibles sont les suivantes : • PIM-DM • PIM-SM
flag	La valeur affichée dans ce champ est valide si le protocole de routage multicast est PIM-SM. Les valeurs possibles sont RPT et SPT. Pour les autres protocoles, un "-----" est affiché.

PIM pour le routage multicast IPv6

Le protocole PIM (Protocol-Independent Multicast) est un protocole de routage multicast standard qui fournit un routage multicast interdomaine évolutif sur Internet, indépendant de tout protocole de routage unicast particulier.

Vous pouvez configurer les différents paramètres PIM pour le routage multicast IPv6 et afficher les statistiques PIM.

Configurez les paramètres IPv6 PIM globaux sur le commutateur

En fonction des besoins de votre réseau IPv6, vous pouvez activer globalement le mode PIM Sparse (PIM-SM) ou le mode PIM dense (PIM-DM) sur le commutateur.

Pour configurer les paramètres IPv6 PIM globaux sur le commutateur :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > Multicast IPv6 > PIM IPv6 > Configuration globale**.

La page Configuration globale s'affiche.

6. Sélectionnez l'un des boutons radio mode Admin suivants :

- Désactiver : Le module PIM est désactivé sur le commutateur. Il s'agit de l'option par défaut.
- **PIM-SM** : Le mode épars PIM est activé sur le commutateur.
- PIM-DM Le mode dense PIM est activé sur le commutateur.

7. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Ajouter des groupes PIM-SSM IPv6

Alors que PIM utilise un routeur de point de rendez-vous (RP) spécialement configuré qui sert de jonction de réunion pour les expéditeurs et les auditeurs de multidiffusion, PIM Single-source Multicast (PIM-SSM) n'utilise pas de point de rendez-vous (RP).

PIM-SSM prend uniquement en charge les arborescences de livraison de route source. informatique est utilisé entre les routeurs (y compris les interfaces de routeur de commutateur) afin qu'ils puissent suivre les paquets de multidiffusion à transmettre les uns aux autres et à leurs réseaux locaux directement connectés. Vous pouvez implémenter PIM-SSM avec un sous-ensemble strict des mécanismes du protocole PIM. La multidiffusion IPv6 régulière et SSM peuvent coexister sur un même routeur, et les deux peuvent être implémentés à l'aide du protocole PIM. Une plage d'adresses multicast, FF3x : :/32 pour IPv6, est réservée au SSM.

Pour ajouter un groupe PIM-SSM IPv6 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.
4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **routage > Multicast IPv6 > PIM IPv6 > Configuration SSM** .
L'écran SSM Configuration (Configuration IP) s'affiche.
6. Dans le champ **adresse du groupe SSM**, entrez l'adresse IPv6 du groupe de multidiffusion spécifique à la source.
7. Dans le champ **masque de groupe SSM**, entrez le préfixe d'adresse IPv6 du groupe de multidiffusion spécifique à la source.
8. Cliquez sur le bouton **Add** (Ajouter).
Les paramètres sont enregistrés. Le groupe est ajouté.
9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimer un groupe PIM-SSM IPv6

Vous pouvez supprimer un groupe PIM-SSM IPv6 dont vous n'avez plus besoin.

Pour supprimer un groupe PIM-SSM IPv6 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routing > Multicast IPv6 > PIM IPv6 > Configuration SSM**.

L'écran SSM Configuration (Configuration IP) s'affiche.

6. Cochez la case correspondant au groupe PIM-SSM.

7. Cliquez sur le bouton **Supprimer**.

Les paramètres sont enregistrés. Le groupe PIM-SSM est supprimé.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurer une interface PIM IPv6

Vous pouvez configurer une interface IPv6 pour PIM.

Pour configurer une interface PIM IPv6 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **roulage > Multicast IPv6 > PIM IPv6 > Configuration de l'interface**.

La page Configuration de l'interface s'affiche.

6. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :

- **1 ou ID d'unité pour un commutateur empilé :**

- 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
 - **ID d'unité pour un commutateur empilé** : Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
 - VLAN Seuls les VLAN sont affichés.
 - **Tous**: Les interfaces physiques et les VLAN sont affichés, ou pour une pile de commutateurs, les interfaces physiques et les VLAN de tous les commutateurs sont affichés.
7. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :
- Pour afficher ou effacer les statistiques d'une seule interface, cochez la case associée à l'interface ou saisissez le numéro de l'interface dans le champ **aller à l'interface** et cliquez sur le bouton **aller**.
 - Pour configurer plusieurs interfaces avec les mêmes paramètres, cochez la case associée à chaque interface.
 - Pour configurer toutes les interfaces avec les mêmes paramètres, cochez la case dans la ligne d'en-tête.
8. Dans le menu **mode Admin**, sélectionnez **Activer** ou **désactiver** pour activer ou désactiver PIM pour l'interface.
La valeur par défaut est désactiver.
9. Dans le champ **intervalle Hello**, spécifiez la période en secondes entre la transmission des messages Hello PIM sur l'interface.
La plage est de 0 à 18000. Le numéro par défaut est 30.
10. Dans le champ **intervalle de jointure/élagage**, spécifiez la période en secondes à laquelle les messages PIM Join/élagage sont transmis sur l'interface.
La plage est de 0 à 18000. Le numéro par défaut est 60.
11. Dans le menu **BSR Border**, sélectionnez **Enable (Activer)** ou **Disable (désactiver)** pour activer ou désactiver la bordure du routeur d'amorçage (BSR) sur l'interface.
La valeur par défaut est désactiver.
12. Dans le champ **priorité DR**, spécifiez la priorité du routeur désigné (DR) pour l'interface.
La plage est de 0 à 2147483647. Le numéro par défaut est 1.
13. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
14. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 142 : Informations de configuration de l'interface PIM IPv6

Champ	Description
État du protocole	État du PIM sur l'interface (opérationnel ou non opérationnel).
Longueur du préfixe IPv6	Adresse IPv6 et longueur du préfixe de l'interface PIM du routeur.
Routeur désigné	Adresse IPv6 du routeur désigné sur l'interface PIM.
Nombre de voisins	Nombre de voisins PIM sur l'interface PIM.

Afficher les voisins PIM IPv6 et rechercher la base de données des voisins PIM

Vous pouvez afficher les informations de voisinage PIM IPv6 et rechercher dans la base de données de voisins PIM par interface ou par adresse IP de voisin.

Pour afficher les voisins PIM IPv6 et effectuer une recherche dans la base de données des voisins PIM :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > Multicast IPv6 > PIM IPv6 > voisin PIM**.

La page de voisinage PIM s'affiche.

6. Pour rechercher des entrées de groupe IGMP par interface ou par groupe, sélectionnez l'une des options suivantes dans le menu **Rechercher** :

- Interface Sélectionnez **interface** dans le menu, spécifiez l'interface au format unité/port (par exemple 0/8), puis cliquez sur le bouton **aller**.
Si l'entrée existe, l'entrée est affichée en tant que première entrée, suivie des entrées restantes.
- IP voisin Sélectionnez **IP voisin** dans le menu, spécifiez l'adresse IPv6 du voisin, puis cliquez sur le bouton **aller**.
Si l'entrée existe, l'entrée avec l'adresse IPv6 voisine correspondante est affichée comme première entrée, suivie des entrées restantes. Une correspondance exacte est requise.

7. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

Le tableau suivant décrit les champs en lecture seule de la page.

Table 143 : Informations de voisinage PIM IPv6

Champ	Description
Interface	Interface sur laquelle le PIM voisin est connecté.
IP voisin	Adresse IPv6 du voisin PIM.
Temps de fonctionnement (hh:mm:ss)	Temps écoulé depuis que le périphérique PIM est devenu un voisin de l'interface.
Heure d'expiration (hh:mm:ss)	Le temps restant avant que le PIM voisin ne vieillisse.
Priorité DR	Priorité de routeur désigné (DR) du voisin PIM.

Ajoutez une configuration de point de rendez-vous candidat PIM IPv6

Vous pouvez ajouter une configuration de point de rendez-vous candidat PIM IPv6 sur une interface.

Pour ajouter une configuration RP candidate PIM IPv6 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > Multicast IPv6 > PIM IPv6 > Configuration RP candidate**.

La page Configuration du RP candidat s'affiche.

6. Dans le menu **interface**, sélectionnez l'interface.

7. Dans le champ **adresse du groupe**, spécifiez l'adresse IPv6 du groupe qui est transmise dans les annonces RP-candidates.

8. Dans le champ **longueur du préfixe**, saisissez la longueur du préfixe IPv6 du groupe qui est transmise dans les annonces RP-candidates.

9. Dans le champ **intervalle d'annonce C-RP**, spécifiez la période en secondes pendant laquelle les annonces RP-candidates sont envoyées en tant que trafic de monodiffusion au routeur d'amorçage (BSR).

La plage est de 1 à 16383 secondes.

10. Cliquez sur le bouton **Add** (Ajouter).

Les paramètres sont enregistrés. Le RP candidat PIM est ajouté.

11. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimer une configuration de point de rendez-vous candidat PIM IPv6

Vous pouvez supprimer une configuration de point de rendez-vous candidat PIM IPv6 dont vous n'avez plus besoin.

Pour supprimer une configuration RP candidate PIM IPv6 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > Multicast IPv6 > PIM IPv6 > Configuration RP candidate**.

La page Configuration du RP candidat s'affiche.

6. Dans le menu **interface**, sélectionnez l'interface.

7. Cochez la case correspondant au RP candidat PIM.

8. Cliquez sur le bouton **Supprimer**.

Les paramètres sont enregistrés. L'entrée RP candidat PIM est supprimée.

Configurez une interface comme candidat routeur d'amorçage PIM IPv6

Vous pouvez configurer une interface en tant que candidat au routeur d'amorçage PIM (BSR) IPv6.

Pour configurer une interface en tant que candidat BSR PIM IPv6 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **roulage > Multicast IPv6 > PIM IPv6 > Configuration candidate BSR**.

La page Configuration du candidat BSR s'affiche.

6. Dans le menu **interface**, sélectionnez une interface.
7. Dans le champ **longueur du masque de hachage**, spécifiez la longueur du masque de hachage à annoncer dans les messages d'amorçage.

La longueur du masque de hachage est utilisée dans l'algorithme de hachage pour sélectionner le RP d'un groupe particulier. La plage est de 0 à 128. Le numéro par défaut est 126.

8. Dans le champ **priorité**, spécifiez la priorité du candidat BSR.
La plage est de 0 à 255. Le numéro par défaut est 0.
9. Dans le champ **intervalle d'annonce**, spécifiez la période en secondes entre les annonces.
La plage est de 1 à 16383. Le numéro par défaut est 60.
10. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
11. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.
12. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).
Le tableau suivant décrit les champs en lecture seule de la page.

Table 144 : Informations de configuration candidate BSR PIM IPv6

Champ	Description
Délai d'expiration BSR (hh:mm:ss)	Durée (en heures, minutes et secondes) après laquelle le BSR sélectionné appréhendé expire.
Adresse IP	Adresse IPv6 du BSR sélectionné.
Message d'amorçage suivant (hh:mm:ss)	Temps (en heures, minutes et secondes) après lequel le prochain message d'amorçage est dû à partir du BSR.
Annonce RP du candidat suivant (hh:mm:ss)	Durée (en heures, minutes et secondes) après laquelle la prochaine annonce RP de candidat est envoyée.

Supprimez une configuration candidate de routeur d'amorçage PIM IPv6

Vous pouvez supprimer une configuration candidate de routeur d'amorçage PIM (BSR) IPv6 d'une interface.

Pour supprimer une configuration candidate BSR PIM IPv6 d'une interface :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > Multicast IPv6 > PIM IPv6 > Configuration candidate BSR**.

La page Configuration du candidat BSR s'affiche.

6. Dans le menu **interface**, sélectionnez l'interface.

7. Cliquez sur le bouton **Supprimer**.

Les paramètres sont enregistrés. La configuration candidate PIM BSR est supprimée de l'interface.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez un point de rendez-vous PIM IPv6 statique pour un groupe

Vous pouvez ajouter un nouveau point de rendez-vous PIM IPv6 statique ou modifier un point de rendez-vous (RP) IPv6 existant pour un groupe.

Pour ajouter ou modifier un PIM RP IPv6 statique pour un groupe :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > Multicast IPv6 > PIM IPv6 > Configuration RP statique** .

La page Configuration RP statique s'affiche.

6. Si vous modifiez un RP statique existant, cochez la case correspondant au RP statique.

7. Dans le champ **adresse RP**, spécifiez l'adresse IPv6 du RP statique.

8. Dans le champ **adresse du groupe**, spécifiez l'adresse IPv6 du groupe auquel s'applique le RP statique.

9. Dans le champ **longueur du préfixe**, spécifiez la longueur du préfixe IPv6 pour le groupe auquel s'applique le RP statique.

10. Dans le menu **Override**, sélectionnez **Enable** ou **Disable** pour activer ou désactiver la capacité de remplacement d'un RP statique sur un RP appris à partir d'un BSR.

Si vous sélectionnez **Activer** et qu'un conflit se produit, un RP statique remplace un RP appris à partir d'un BSR.

11. Effectuez l'une des opérations suivantes :

- Si vous ajoutez un nouveau RP statique, cliquez sur le bouton **Ajouter**.
Les paramètres sont enregistrés. Le RP statique est ajouté.
- Si vous modifiez un RP statique existant, cliquez sur le bouton **appliquer**.

Les paramètres sont enregistrés.

12. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimez une configuration de point de rendez-vous PIM IPv6 statique

Vous pouvez supprimer une configuration de point de rendez-vous (RP) PIM IPv6 statique dont vous n'avez plus besoin pour un groupe.

Pour supprimer une configuration PIM RP IPv6 statique pour un groupe :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur principale à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **roulage > Multicast IPv6 > PIM IPv6 > Configuration RP statique** .

La page Configuration RP statique s'affiche.

6. Cochez la case du RP statique.

7. Cliquez sur le bouton **Supprimer**.

Les paramètres sont enregistrés. La configuration RP statique est supprimée pour le groupe.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

MLD pour le routage multicast IPv6

Vous pouvez configurer les paramètres MLD (Multicast Listener Discovery) et afficher les statistiques MLD.

MLD est un protocole utilisé par les routeurs multicast IPv6 pour découvrir la présence d'auditeurs multicast (nœuds configurés pour recevoir des paquets multicast IPv6) sur ses liens directement attachés et pour découvrir quels paquets multicast sont d'intérêt pour les nœuds voisins. MLD est dérivé de IGMP ; MLD version 1 (MLDv1) est équivalent à IGMPv2, et MLD version 2 (MLDv2) est équivalent à IGMPv3. MLD est un sous-protocole du protocole ICMPv6 (Internet Control message Protocol version 6), et les messages MLD sont un sous-ensemble de messages ICMPv6, identifiés dans les paquets IPv6 par une valeur d'en-tête suivant précédente de 58.

Le commutateur peut surveiller les paquets de protocole MLDv1 et MLDv2 et ponter les données de multidiffusion IPv6 en fonction des adresses MAC de multidiffusion IPv6 de destination. Le commutateur peut prendre en charge la surveillance MLD et igmp snooping simultanément.

Configurez les paramètres MLP globaux du commutateur

Vous pouvez configurer les paramètres MLDP globaux du commutateur, par opposition aux paramètres MLD d'une interface.

Pour configurer les paramètres MLP globaux du commutateur :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > Multicast IPv6 > MLD > Configuration globale** .

La page Configuration globale s'affiche.

6. Sélectionnez le bouton radio **Activer** ou **désactiver** le mode Admin pour activer ou désactiver le MLD sur le commutateur.

La valeur par défaut est désactiver.

7. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurer une interface de routage MLD

Vous pouvez configurer une ou plusieurs interfaces de routage MLD.

Pour configurer une interface de routage MLD :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > Multicast IPv6 > MLD > Configuration de l'interface de routage**.

La page Configuration de l'interface de routage s'affiche.

6. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :

- **1 ou ID d'unité pour un commutateur empilé :**
 - 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
 - **ID d'unité pour un commutateur empilé :** Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
- **VLAN** Seuls les VLAN sont affichés.
- **Tous:** Les interfaces physiques et les VLAN sont affichés, ou pour une pile de commutateurs, les interfaces physiques et les VLAN de tous les commutateurs sont affichés.

7. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :

- Pour afficher ou effacer les statistiques d'une seule interface, cochez la case associée à l'interface ou saisissez le numéro de l'interface dans le champ **aller à l'interface** et cliquez sur le bouton **aller**.
 - Pour configurer plusieurs interfaces avec les mêmes paramètres, cochez la case associée à chaque interface.
 - Pour configurer toutes les interfaces avec les mêmes paramètres, cochez la case dans la ligne d'en-tête.
8. Dans le menu **mode Admin**, sélectionnez **Activer** ou **désactiver** pour activer ou désactiver MLD pour l'interface.
La valeur par défaut est désactiver.
 9. Dans le champ **version**, spécifiez la version de MLD pour l'interface.
La version peut être V1 ou V2. La valeur par défaut est V2.
 10. Dans le champ **intervalle de requête**, entrez la fréquence en secondes à laquelle les paquets de requête hôte MLD doivent être transmis sur l'interface.
La valeur est comprise entre 1 et 3600. Le numéro par défaut est 125.
 11. Dans le champ **Query Max Response Time**, entrez le temps de réponse maximal de requête, en millisecondes, à annoncer dans les requêtes MLDv2 sur l'interface.
La valeur est comprise entre 0 et 65535. La valeur par défaut est de 10000 millisecondes.
 12. Dans le champ **intervalle de requête de démarrage**, entrez le nombre de secondes entre la transmission des requêtes de démarrage sur l'interface.
La valeur est comprise entre 1 et 300. Le numéro par défaut est 31.
 13. Dans le champ **nombre de requêtes de démarrage**, entrez le nombre de requêtes à envoyer au démarrage, séparées par l'intervalle de requête de démarrage.
La valeur est comprise entre 1 et 20. Le numéro par défaut est 2.
 14. Dans le champ **intervalle de requête du dernier membre**, entrez l'intervalle de requête du dernier membre en millisecondes.
Cette valeur est le temps de réponse maximal à insérer dans les requêtes spécifiques au groupe envoyées en réponse aux messages Leave Group, et est également la période entre les messages de requête spécifiques au groupe. La valeur est comprise entre 0 et 65535. La valeur par défaut est de 1000 millisecondes.
 15. Dans le champ **nombre de requêtes du dernier membre**, entrez le nombre de requêtes à envoyer lors de la réception d'un rapport de groupe de congés.
La valeur est comprise entre 1 et 20. Le numéro par défaut est 2.
 16. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

17. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 145 : Configuration de l'interface de routage MLD

Champ	Description
Mode de fonctionnement	État opérationnel du MLD sur l'interface.
Robustesse	Paramètre de robustesse de l'interface. La valeur par défaut est 2.

Afficher les statistiques des interfaces de routage MLD

Vous pouvez afficher les statistiques des interfaces de routage MLD.

Pour afficher les statistiques des interfaces de routage MLD :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > Multicast IPv6 > MLD > statistiques de l'interface de routage**.

La page statistiques de l'interface de routage s'affiche.

6. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :

- **1 ou ID d'unité pour un commutateur empilé :**
 - 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
 - **ID d'unité pour un commutateur empilé :** Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
- **VLAN** Seuls les VLAN sont affichés.
- **Tous:** Les interfaces physiques et les VLAN sont affichés, ou pour une pile de commutateurs, les interfaces physiques et les VLAN de tous les commutateurs sont affichés.

7. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

Le tableau suivant décrit les champs en lecture seule de la page.

Table 146 : Informations statistiques de l'interface de routage MLD

Champ	Description
Interface	Interface sur laquelle MLD est activé.
Statut Querier	Indique si l'interface est un interrogateur MLD ou non sur le sous-réseau IPv6 auquel informatique est associé.
Querier IP	Adresse IPv6 du interrogateur MLD sur le sous-réseau IPv6 auquel l'interface est rattachée.
Querier Up Time	Période en secondes depuis la dernière modification du questionneur d'interface MLD.
Délai d'expiration du Querier	La période en secondes restante avant l'expiration de l'autre temporisateur de présence de l'interrogateur. Si le commutateur est l'interrogateur, cela vaut zéro.
Requêtes de version erronées reçues	Nombre de requêtes reçues sur l'interface avec une version MLD qui ne correspond pas à la version MLD configurée pour l'interface
Nombre de joints reçus	Nombre de fois qu'une appartenance à un groupe a été ajoutée sur l'interface, c'est-à-dire le nombre de fois qu'une entrée pour l'interface a été ajoutée à la table de cache.
Nombre de groupes	Nombre actuel d'entrées pour l'interface dans la table cache.

Affichez les groupes MLD et effectuez une recherche dans la base de données des groupes MLD

Vous pouvez afficher les informations du groupe MLD et effectuer une recherche dans la base de données des groupes MLD par interface ou par groupe.

Pour afficher les groupes MLD et effectuer une recherche dans la base de données des groupes MLD :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routing > Multicast IPv6 > MLD > groupes MLD**.

La page groupes MLD s'affiche.

6. Pour rechercher des entrées de groupe IGMP par interface ou par groupe, sélectionnez l'une des options suivantes dans le menu **Rechercher** :

- Interface Sélectionnez **interface** dans le menu, spécifiez l'interface au format unité/port (par exemple 0/8), puis cliquez sur le bouton **aller**.
Si l'entrée existe, l'entrée est affichée en tant que première entrée, suivie des entrées restantes.
- Groupe Sélectionnez **Groupe** dans le menu, spécifiez l'adresse IPv6 du groupe de multidiffusion, puis cliquez sur le bouton **aller**.
Si l'entrée existe, l'entrée avec l'adresse IPv6 de groupe correspondante est affichée comme première entrée, suivie des entrées restantes. Une correspondance exacte est requise.

7. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

Le tableau suivant décrit les champs en lecture seule de la page.

Table 147 : MLD regroupe les informations

Champ	Description
Interface	Interface sur laquelle MLD est activé.
IP du groupe	Adresse du groupe de multidiffusion IP.
Dernier reporter	Adresse IP de la source du dernier rapport d'appartenance reçu pour l'adresse du groupe de multidiffusion IP sur l'interface.
Durée de fonctionnement	Période écoulée depuis la création de cette entrée.
Heure d'expiration	Période restante avant expiration de cette entrée.
Mode de filtrage	Le mode de filtre source (inclure, exclure ou NA) pour le groupe sur l'interface. Si le mode est NA, le champ est vide.
Temporisateur hôte version 1	Période restante jusqu'à ce que le commutateur détermine qu'aucun membre MLD version 1 n'est attaché à l'interface.
Mode compat. Groupe	Le mode de compatibilité (MLDv1 ou MLDv2) du groupe multicast sur l'interface.
Hôtes sources	Adresses sources membres de l'adresse multicast.
Adresse source (heure d'expiration)	Délai d'expiration après lequel chaque adresse source membre du groupe de multidiffusion expire.

Afficher ou effacer les statistiques de trafic MLD

Vous pouvez afficher les statistiques de trafic MLD et effacer ces statistiques.

Pour afficher ou effacer les statistiques de trafic MLD IPv6 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routing > Multicast IPv6 > MLD > trafic MLD**.

La page trafic MLD s'affiche.

6. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).
7. Pour réinitialiser (effacer) toutes les statistiques de trafic MLD, cliquez sur le bouton **Effacer**.
8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 148 : Informations statistiques de trafic MLD

Champ	Description
Paquets MLD valides reçus	Nombre de paquets MLD valides reçus sur l'interface.
Paquets MLD valides envoyés	Nombre de paquets MLD valides envoyés par le commutateur.

Table 148 : Informations statistiques de trafic MLD (A continué)

Champ	Description
Requêtes reçues	Nombre de requêtes MLD valides reçues par le commutateur.
Requêtes envoyées	Nombre de requêtes MLD valides envoyées par le commutateur.
Rapports reçus	Nombre de rapports MLD valides reçus par le commutateur.
Rapports envoyés	Nombre de rapports MLD valides envoyés par le commutateur.
Congés reçus	Le nombre de messages MLD Leave valides reçus par le commutateur.
Feuilles envoyées	Le nombre de messages MLD Leave valides envoyés par le commutateur.

Configurer une interface proxy MLD

Vous pouvez configurer une interface proxy MLD. Les exigences suivantes s'appliquent :

- Le routage, le MLD et la multidiffusion doivent être globalement activés sur le commutateur.
- Vous devez configurer au moins une interface de routage.
- L'interface proxy MLD ne peut pas être la même qu'une interface de routage MLD.

Pour configurer une interface proxy MLD :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > Multicast IPv6 > MLD > Configuration de l'interface proxy**.

La page Configuration de l'interface proxy s'affiche.

6. Dans le menu **interface**, sélectionnez l'interface qui doit fonctionner comme interface proxy IGMP.

7. Dans le menu **mode Admin**, sélectionnez **Activer** ou **désactiver** pour activer ou désactiver la fonction proxy IGMP sur l'interface.

La valeur par défaut est désactiver.

8. Dans le champ **intervalle de rapport non sollicité**, spécifiez la période en secondes entre les répétitions du rapport initial d'un hôte sur l'appartenance à un groupe.

La plage est de 1 à 260. Le numéro par défaut est 1.

9. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 149 : Informations de configuration de l'interface proxy MLD

Champ	Description
Préfixe IPv6	Adresse IPv6 de l'interface proxy MLD.
Longueur de préfixe	Longueur du préfixe de l'adresse IPv6 de l'interface proxy MLD.
Mode de fonctionnement	État opérationnel de l'interface proxy IGMP (désactiver ou Activer).
Adresse du Querier sur l'interface proxy	Adresse de l'interrogeur sur l'interface proxy.

Table 149 : Informations de configuration de l'interface proxy MLD (A continué)

Champ	Description
Nombre de groupes	Nombre d'entrées de groupe de multidiffusion pour l'interface proxy MLD dans la table cache.
Version	Version de MLD configurée sur l'interface de routage MLD que vous avez modifiée en interface proxy MLD. Pour plus d'informations, consultez la section Configurer une interface de routage MLD à la page 749.
Expiration du délai du Querier version 1	Délai d'expiration du interrogateur MLDv1 en secondes. Si un hôte reçoit une requête MLDv1, il définit temporairement son temporisateur de présence de requête MLDv1 sur l'intervalle de requête MLDv1. Une fois que l'hôte a lu la requête MLDv1, le délai d'expiration du questionneur MLDv1 indique la période après laquelle l'hôte repasse à MLDv2.
Fréquence de démarrage du proxy	Le nombre de fois où le proxy a été démarré.

Afficher les statistiques de l'interface proxy MLD

Vous pouvez afficher les statistiques de l'interface proxy MLD.

Pour afficher les statistiques de l'interface proxy MLD :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > Multicast IPv6 > MLD > statistiques de l'interface proxy**.

La page statistiques de l'interface proxy s'affiche.

6. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

Le tableau suivant décrit les champs en lecture seule de la page.

Table 150 : Informations statistiques sur l'interface proxy MLD

Champ	Description
Interface proxy	Interface sur laquelle les paquets proxy MLD sont reçus.
Version	Version des paquets proxy MLD reçus.
Requêtes reçues	Nombre de requêtes proxy MLD reçues.
Rapports reçus	Nombre de rapports proxy MLD reçus.
Rapports envoyés	Nombre de rapports proxy MLD envoyés.
Congés reçus	Le nombre de messages de congé de proxy MLD reçus.
Feuilles envoyées	Le nombre de messages de congé de proxy MLD envoyés.

Affichez l'appartenance au proxy MLD et recherchez dans la base de données d'appartenance au proxy MLD

Vous pouvez afficher les informations d'appartenance au proxy MLD et rechercher la base de données d'appartenance au proxy MLD par groupe.

Pour afficher les informations d'appartenance au proxy MLD et effectuer une recherche dans la base de données d'appartenance au proxy MLD :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > Multicast IPv6 > MLD > Proxy Membership**.

La page adhésion au proxy s'affiche.

6. Pour rechercher l'appartenance à un proxy MLD par groupe, spécifiez l'adresse IPv6 du groupe de multidiffusion, puis cliquez sur le bouton **aller**.

Si l'entrée existe, l'entrée avec l'adresse IPv6 de groupe correspondante est affichée comme première entrée, suivie des entrées restantes. Une correspondance exacte est requise.

7. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

Le tableau suivant décrit les champs en lecture seule de la page.

Table 151 : Informations sur l'appartenance au proxy MLD

Champ	Description
Interface proxy	Interface sur laquelle le proxy MLD est activé.
IP du groupe	Adresse du groupe de multidiffusion IPv6.
Hôtes sources	Adresses sources membres du groupe multicast.
Dernier reporter	Adresse IPv6 source qui a envoyé le dernier rapport d'appartenance pour le groupe de multidiffusion sur l'interface proxy MLD.
Durée de fonctionnement	Temps écoulé depuis la création de cette entrée.
Heure d'expiration	Intervalle d'expiration de chaque adresse source membre du groupe de multidiffusion. Il s'agit de la période au bout de laquelle l'entrée de la source expire.
Etat	État de l'entrée hôte : • Etat non membre : L'hôte n'appartient pas au groupe sur l'interface. • Retarder l'État membre : L'hôte appartient au groupe sur l'interface et son temporisateur de rapport est actif. (La minuterie de rapport est utilisée pour envoyer des rapports.) • Etat membre inactif : L'hôte appartient au groupe sur l'interface mais son temporisateur de rapport est inactif.
Mode de filtrage	Mode de filtre de groupe (inclure, exclure ou aucun) pour le groupe sur l'interface proxy MLD.
Nombre de sources	Nombre d'hôtes source dans le groupe de multidiffusion.

Routes de multidiffusion statiques pour les adresses IPv6

Si un protocole de routage multicast tel que PIM-SM ou PIM-DM est activé et configuré, les routes multicast sont construites dynamiquement. Toutefois, vous pouvez également configurer une ou plusieurs routes de multidiffusion IPv6 statiques. Une route statique peut faciliter le traitement du trafic de multidiffusion lorsqu'un routeur de redirection de chemin inverse (RPF) voisin est situé entre le commutateur et la source de multidiffusion.

Configurer des routes de multidiffusion statiques pour les adresses IPv6

Vous pouvez ajouter une nouvelle route de multidiffusion IPv6 statique ou modifier une route existante.

Pour ajouter ou modifier une route de multidiffusion IPv6 statique :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **roulage > Multicast IPv6 > Configuration des routes statiques** .

La page Configuration des routes statiques s'affiche.

6. Si vous modifiez une route de multidiffusion statique existante, cochez la case de la route.

Pour une route statique existante, vous pouvez uniquement modifier la métrique.

7. Dans le champ **IP source**, spécifiez l'adresse IPv6 de la source du paquet multicast.
8. Dans le champ **longueur du préfixe**, spécifiez la longueur du préfixe IPv6 de la source du paquet de multidiffusion.

9. Dans le champ **voisin RPF**, spécifiez l'adresse IPv6 du routeur RPF voisin situé entre le commutateur et la source de multidiffusion.
10. Dans le champ **métrique**, spécifiez le coût de l'état de la liaison du chemin de la source de multidiffusion au commutateur.
La plage est de 0 à 255.
11. Dans le menu **interface RPF**, sélectionnez l'interface connectée au voisin RPF.
12. Effectuez l'une des opérations suivantes :
 - Si vous ajoutez une nouvelle route de multidiffusion statique, cliquez sur le bouton **Ajouter**.
Les paramètres sont enregistrés. La route de multidiffusion statique est ajoutée.
 - Si vous modifiez une route de multidiffusion statique existante, cliquez sur le bouton **appliquer**.
Les paramètres sont enregistrés.
13. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimer une route de multidiffusion statique pour une adresse IPv6

Vous pouvez supprimer une route de multidiffusion IPv6 statique dont vous n'avez plus besoin.

Pour supprimer une route de multidiffusion statique :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **routage > Multicast IPv6 > Configuration des routes statiques**.

La page Configuration des routes statiques s'affiche.

6. Cochez la case de la route statique.

7. Cliquez sur le bouton **Supprimer**.

Les paramètres sont enregistrés. La route statique est supprimée.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

8

Configurer la qualité de service

Ce chapitre aborde les sujets suivants :

- Concepts de qualité de service.
- Classe de service
- Services différenciés

Concepts de qualité de service.

Dans un commutateur, chaque port physique est constitué d'une ou plusieurs files d'attente pour la transmission de paquets sur le réseau connecté. Plusieurs files d'attente par port sont souvent fournies pour donner la préférence à certains paquets par rapport à d'autres en fonction de critères définis par l'utilisateur. Lorsqu'un paquet est mis en file d'attente pour transmission dans un port, la vitesse à laquelle il est desservi dépend de la façon dont la file d'attente est configurée et éventuellement de la quantité de trafic présente dans les autres files d'attente du port. Si un délai est nécessaire, les paquets sont conservés dans la file d'attente jusqu'à ce que l'ordonnanceur autorise la transmission de la file d'attente. Lorsque les files d'attente deviennent pleines, les paquets ne peuvent plus être retenus pour la transmission et sont abandonnés par le commutateur.

La qualité de service est un moyen d'obtenir une transmission de données prévisible et cohérente en distinguant les paquets dont les exigences temporelles sont strictes de ceux qui tolèrent plus facilement les retards. Les paquets avec des exigences de synchronisation strictes reçoivent un traitement spécial dans un réseau compatible QoS. Dans cet esprit, tous les éléments du réseau doivent être compatibles QoS. La présence d'au moins un nœud qui n'est pas compatible QoS crée une déficience dans le chemin du réseau, et les performances de l'ensemble du flux de paquets sont compromises.

Classe de service

La fonction de mise en file d'attente de classe de service (cos) vous permet de configurer directement certains aspects de la mise en file d'attente de commutateur. Cela fournit le comportement QoS souhaité pour différents types de trafic réseau lorsque les complexités de DiffServ ne sont pas requises. La priorité d'un paquet arrivant à une interface peut être utilisée pour diriger le paquet vers la file d'attente cos sortante appropriée par l'intermédiaire d'une table de mappage. Les caractéristiques de file d'attente CS qui affectent le mappage de file d'attente, telles que la bande passante minimale garantie ou la mise en forme du débit de transmission, peuvent être configurées par l'utilisateur au niveau de la file d'attente (ou du port).

Huit files d'attente par port sont prises en charge.

Concepts de configuration cos .

Vous pouvez définir le mode de confiance classe de service pour une interface. Chaque port du commutateur peut être configuré pour approuver l'un des champs de paquets (802.1p ou IP DSCP), ou pour ne pas approuver la désignation de priorité d'un paquet

(mode non approuvé). Si le port est défini sur un mode approuvé, informatique utilise une table de mappage appropriée pour le champ approuvé utilisé. Cette table de mappage indique la file d'attente cos vers laquelle le paquet doit être transféré sur le port de sortie approprié. Bien entendu, le champ de confiance doit exister dans le paquet pour que la table de mappage soit utile. Si ce n'est pas le cas, des actions par défaut sont effectuées. Ces actions impliquent de diriger le paquet vers un niveau cos spécifique configuré pour le port d'entrée dans son ensemble, en fonction de la priorité par défaut du port existant telle qu'elle est mappée à une classe de trafic par la table de mappage 802.1p actuelle.

Alternativement, lorsqu'un port est configuré comme non approuvé, informatique ne fait confiance à aucune désignation de priorité de paquet entrant et utilise la valeur de priorité par défaut du port à la place. Tous les paquets arrivant à l'entrée d'un port non sécurisé sont dirigés vers une file d'attente cos spécifique sur les ports de sortie appropriés, conformément à la priorité par défaut configurée du port d'entrée. Ce processus est également utilisé dans les cas où un mappage de port approuvé ne peut pas être honoré, par exemple lorsqu'un paquet non IP arrive à un port configuré pour approuver la valeur DSCP IP.

Configurez les paramètres du mode de confiance cos globalement ou pour une interface spécifique

Un paramètre de configuration du mode de confiance cos global est appliqué à toutes les interfaces du commutateur.

Un paramètre de configuration du mode de confiance cos pour une interface est appliqué à l'interface sélectionnée uniquement. Pour configurer le mode de confiance cos pour plusieurs interfaces, répétez la tâche pour chaque interface sélectionnée.

Pour configurer les paramètres du mode de confiance cos sur toutes les interfaces ou sur une interface spécifique :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **QoS > cos > basique > Configuration cos**.

La page Configuration cos s'affiche.

6. Configurez les mêmes paramètres de mode de confiance cos pour toutes les interfaces configurables par cos ou configurez les paramètres cos par interface.

Par défaut, le bouton radio Ethernet est sélectionné.

- Pour configurer les mêmes paramètres de mode de confiance de classe de service pour toutes les interfaces configurables de classe de service, procédez comme suit :
 - a. Sélectionnez le bouton radio **Global**.
 - b. Dans le menu **Global Trust mode**, sélectionnez l'une des options de mode Trust suivantes pour le trafic entrant sur le commutateur :
 - **non fiable** : Ne faites confiance à aucun marquage de paquet cos à l'entrée.
 - **trust dot1p** : Les huit balises de priorité spécifiées dans IEEE 802.1p sont p0 à p7. Le paramètre QoS vous permet de mapper chacun des huit niveaux de priorité à l'une des huit files d'attente de priorité matérielle internes.
 - **Trust IP-DSCP** : Les six bits les plus significatifs du champ DiffServ sont appelés bits DSCP (Differentiated services Code point). Le mode par défaut est IP-DSCP.
- Pour configurer les paramètres cos d'une interface, procédez comme suit :
 - a. Sélectionnez le bouton radio **interface**.
 - b. Dans le menu interface, sélectionnez l'interface.

Les paramètres configurés s'appliquent uniquement à l'interface sélectionnée.

- c. Dans le menu **interface Trust mode**, sélectionnez l'une des options de mode Trust suivantes :
 - o **non fiable** : Ne faites confiance à aucun marquage de paquet cos à l'entrée.
 - o **trust dot1p** : Les huit balises de priorité spécifiées dans IEEE 802.1p sont p0 à p7. Le paramètre QoS vous permet de mapper chacun des huit niveaux de priorité à l'une des sept files d'attente de priorité matérielle internes.
 - o **Trust IP-DSCP** : Les six bits les plus significatifs du champ DiffServ sont appelés bits DSCP (Differentiated services Code point). Le mode par défaut est IP-DSCP.

7. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Mapper les priorités 802.1p aux files d'attente .

Vous pouvez afficher ou modifier les classes de trafic interne mappées sur les valeurs de classe de priorité 802.1p dans les trames Ethernet que l'unité reçoit. Les mappages de classe priorité-traffic peuvent être appliqués globalement (à toutes les interfaces) ou à chaque interface individuelle. Le mappage permet au commutateur de regrouper différents types de trafic (par exemple, données ou voix) en fonction de leurs exigences de latence et de donner la préférence au trafic sensible au temps.

Pour mapper les priorités 802.1p aux files d'attente pour toutes les interfaces ou interfaces individuelles :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **QoS > cos > Avancé > mappage de file d'attente 802.1p**.

La page mappage de file d'attente 802.1p s'affiche.

6. Dans le menu **interface**, sélectionnez **tout** pour appliquer le mappage à toutes les interfaces ou sélectionnez une interface individuelle.

7. Dans le tableau 802.1p vers la table de mappage de file d'attente, mappez chacune des huit priorités 802.1p à une file d'attente (classe de trafic interne) de **0** à **6**.

La ligne priorité 802.1p contient des sélecteurs de classe de trafic pour chacune des huit priorités 802.1p à mapper. La priorité passe de faible (0) à élevée (7). Par exemple, le trafic avec une priorité de 0 concerne la plupart du trafic de données et est envoyé en utilisant le meilleur effort. Le trafic avec une priorité plus élevée, telle que 7, peut être un trafic sensible au temps, comme la voix ou la vidéo.

Table 152 : Valeurs par défaut pour 802.1p vers le mappage de file d'attente

priorité 802.1p.	0	1	2	3	4	5	6	7
File d'attente par défaut	1	0	0	1	2	2	3	3

Les valeurs du menu sous chaque priorité représentent la classe de trafic. La classe de trafic est la file d'attente matérielle d'un port. Des valeurs de classe de trafic plus élevées indiquent une position de file d'attente plus élevée. Avant d'envoyer le trafic dans une file d'attente inférieure, informatique doit attendre que le trafic dans les files d'attente supérieures soit envoyé.

8. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Mappez les valeurs DSCP aux files d'attente.

Vous pouvez mapper une classe de trafic interne à une valeur DSCP.

Pour mapper les valeurs DSCP aux files d'attente :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **QoS > cos > Avancé > mappage de file d'attente IP DSCP**.

La page IP DSCP queue Mapping s'affiche.

Le champ IP DSCP affiche une valeur IP DSCP comprise entre 0 et 63.

6. Pour chaque valeur DSCP, spécifiez la classe de trafic interne pour mapper la file d'attente correspondante.

7. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez les paramètres de file d'attente cos pour une interface.

Vous pouvez configurer le mode de confiance pour une ou plusieurs interfaces et appliquer un taux de mise en forme d'interface à toutes les interfaces ou à une interface spécifique.

Pour configurer les paramètres cos d'une interface :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **QoS > cos > Avancé > cos interface Configuration**.

La page Configuration de l'interface cos s'affiche.

6. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :

- **1 ou ID d'unité pour un commutateur empilé :**

- 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
 - **ID d'unité pour un commutateur empilé** : Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
 - LAG Seuls les LAG sont affichés.
 - **Tous**: Les interfaces physiques et les LAG sont affichés, ou pour une pile de commutateurs, les interfaces physiques de tous les commutateurs de la pile et les LAG sont affichés.
7. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :
- **Pour configurer une interface unique, cochez la case associée au port ou tapez le numéro de port (par exemple g1) dans le champ aller à l'interface et cliquez sur le bouton aller.**
 - Pour configurer plusieurs interfaces avec les mêmes paramètres, cochez la case associée à chaque interface.
 - Pour configurer toutes les interfaces avec les mêmes paramètres, cochez la case dans la ligne d'en-tête.
8. Dans le menu **interface Trust mode**, sélectionnez l'une des options de mode Trust suivantes pour le trafic entrant sur les interfaces sélectionnées :
- **Non fiable** Ne faites confiance à aucun marquage de paquet cos à l'entrée.
 - **802.1p** : Les huit balises de priorité spécifiées dans IEEE 802.1p sont p0 à p7. Le paramètre QoS vous permet de mapper chacun des huit niveaux de priorité à l'une des sept files d'attente de priorité matérielle internes. La valeur par défaut est 802.1p.
 - **IP-DSCP** : Les six bits les plus significatifs du champ DiffServ sont appelés bits DSCP (Differentiated services Code point).
9. Dans le champ **interface Shaping Rate**, spécifiez la bande passante maximale du débit de transmission sortant en kbps.
- Ce paramètre est utilisé pour façonner le débit de transmission sortant par incréments de 1 % dans une plage de 0 à 100. Cette valeur est contrôlée indépendamment de toute configuration de bande passante maximale par file d'attente. Informatique est effectivement un mécanisme de mise en forme de deuxième niveau. La valeur par défaut est 0. La valeur 0 signifie que le maximum est illimité.
10. Cliquez sur le bouton **Apply** (Appliquer).
- Les paramètres sont enregistrés.
11. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez les paramètres de file d'attente cos pour une interface.

Vous pouvez définir ce qu'une file d'attente particulière fait en configurant des files d'attente de sortie de commutateur. Vous pouvez contrôler la quantité de bande passante utilisée par la file d'attente, la profondeur de la file d'attente pendant les périodes d'encombrement et la planification de la transmission de paquets à partir de toutes les files d'attente d'un port. Chaque port contient sa propre configuration liée à la file d'attente cos.

Pour plus d'informations sur la configuration globale des paramètres de file d'attente cos, reportez-vous à la section [Configurez les paramètres du mode de confiance cos globalement ou pour une interface spécifique](#) à la page 768.

Configurez les paramètres de file d'attente cos pour une interface.

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **QoS > cos > Avancé > Configuration de file d'attente d'interface** .

La page Configuration de la file d'attente d'interface s'affiche.

6. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :
 - **1 ou ID d'unité pour un commutateur empilé :**
 - 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
 - **ID d'unité pour un commutateur empilé :** Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
 - LAG Seuls les LAG sont affichés.
 - **Tous:** Les interfaces physiques et les LAG sont affichés, ou pour une pile de commutateurs, les interfaces physiques de tous les commutateurs de la pile et les LAG sont affichés.
7. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :
 - **Pour configurer une interface unique, cochez la case associée au port ou tapez le numéro de port (par exemple g1) dans le champ aller à l'interface et cliquez sur le bouton aller.**
 - Pour configurer plusieurs interfaces avec les mêmes paramètres, cochez la case associée à chaque interface.
 - Pour configurer toutes les interfaces avec les mêmes paramètres, cochez la case dans la ligne d'en-tête.
8. Dans le menu **ID de file d'attente**, sélectionnez la file d'attente.

Vous pouvez sélectionner une file d'attente de **0 à 6**. (Pour les cos, la file d'attente 7 est réservée à l'empilement.)
9. Dans le champ **bande passante minimale**, spécifiez la bande passante minimale garantie allouée à la file d'attente sur l'interface.

Si vous définissez cette valeur sur une valeur supérieure à la largeur de bande maximale correspondante, la valeur maximale est automatiquement augmentée à la même valeur. La valeur par défaut est 0. La plage est comprise entre 0 et 100 par incréments de 1. La valeur 0 signifie qu'aucune bande passante minimale garantie n'est appliquée. La somme des valeurs de largeur de bande minimale individuelles pour toutes les files d'attente sur l'interface sélectionnée ne peut pas dépasser le maximum (100).

Le paramètre s'applique uniquement à la file d'attente que vous sélectionnez dans le menu **ID de file d'attente**.
10. Dans le menu **type de planificateur**, sélectionnez le type de planification utilisé pour la file d'attente sur l'interface :

- **Strict** : L'interface dessert en premier le trafic ayant la priorité la plus élevée sur une file d'attente.
- **Poids** : L'interface utilise la permutation circulaire pondérée pour associer un poids à chaque file d'attente. Il s'agit de l'option par défaut.

Le paramètre s'applique uniquement à la file d'attente que vous sélectionnez dans le menu **ID de file d'attente**.

11. Dans le menu **type de gestion de file d'attente**, sélectionnez la méthode de gestion de profondeur de file d'attente utilisée pour la file d'attente sur l'interface :

- **TailDrop** : La méthode Taildrop entraîne l'abandon des paquets si la file d'attente est pleine. Lorsque de l'espace devient disponible dans la file d'attente, les paquets sont à nouveau acceptés. Il s'agit de la méthode par défaut.
- **WRED** : La méthode WRED (Weighted Random Early Detection) vous permet d'affiner la gestion des files d'attente de sorte que les paquets soient abandonnés de manière sélective (voir [Configurez les paramètres de priorité cos WRED pour l'abandon de paquets](#) à la page 777).

Le paramètre s'applique uniquement à la file d'attente que vous sélectionnez dans le menu **ID de file d'attente**.

12. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

13. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez les paramètres de priorité cos WRED pour l'abandon de paquets

Si vous utilisez la méthode WRED (Weighted Random Early Detection) comme méthode de gestion de la profondeur de la file d'attente (voir [Configurez les paramètres de file d'attente cos pour une interface](#), à la page 775), vous pouvez configurer les paramètres de priorité pour supprimer des paquets si une file d'attente est pleine. Ces paramètres s'appliquent à une interface sélectionnée et à une file d'attente sélectionnée. Vous pouvez configurer des paramètres différents pour chaque file d'attente et pour chaque niveau de priorité sur une interface.

Pour configurer les paramètres de priorité cos WRED pour l'abandon de paquets :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **QoS > cos > Avancé > cos queue Drop Precedence Configuration**.

La page Configuration de la priorité de DROP de file d'attente cos s'affiche.

6. Dans le menu **interface**, sélectionnez une interface.

7. Dans le menu **queue ID (ID de file d'attente)**, sélectionnez une file d'attente de **0** à **6**. (Pour les cos, la file d'attente 7 est réservée à l'empilement.)

8. Dans le menu **DROP Priedence Level (niveau de priorité de DROP)**, sélectionnez les niveaux de priorité de DROP de **1** à **4**.

Les paquets auxquels s'applique le niveau 1 sont les plus susceptibles d'être abandonnés. Les paquets auxquels s'applique le niveau 4 sont les moins susceptibles d'être abandonnés.

Le tableau suivant indique les valeurs par défaut pour chaque niveau de priorité de DROP. Vous pouvez modifier ces paramètres.

Table 153 : Valeurs par défaut pour les niveaux de priorité de DROP

Supprimer le niveau de priorité	Seuil minimum WRED	Seuil maximum WRED	Échelle de probabilité de chute WRED
1	40	100	10
2	30	90	10
3	20	80	10
4	99	100	10

- Dans le champ **WRED minimum Threshold**, spécifiez le seuil minimum de file d'attente WRED en dessous duquel aucun paquet n'est abandonné pour le niveau de priorité de DROP sélectionné.

La plage est de 0 à 100.

- Dans le champ **WRED maximum Threshold**, spécifiez le seuil maximal de file d'attente ROUGE pondéré au-dessus duquel tous les paquets sont abandonnés pour le niveau de priorité de DROP actuel.

La plage est de 0 à 100.

- Utiliser le champ **échelle de probabilité de chute WRED**, spécifiez la probabilité de chute de paquet pour le niveau de priorité de chute actuel.

La plage est de 0 à 100.

- Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

- Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 154 : État de priorité de suppression de file d'attente de l'interface cos

Champ	Description
Interface	L'interface cos.
ID de file d'attente	ID de la file d'attente.
Niveau de priorité de DROP	Le niveau de priorité de la suppression.
Seuil minimum WRED	Valeur du seuil de file d'attente minimum WRED.
Seuil maximum WRED	La valeur maximale du seuil de file d'attente WRED.
Échelle de probabilité de chute WRED	La valeur de probabilité de perte de paquet WRED.

Services différenciés

La fonctionnalité QoS contient la prise en charge des services différenciés (DiffServ) qui permet de classer le trafic en flux et de lui donner un certain traitement QoS conformément aux comportements par saut définis.

Les réseaux IP standard fournissent un service de livraison de données optimal. Le service Best effort implique que le réseau livre les données en temps opportun, bien qu'il n'y ait aucune garantie. En cas de congestion, les paquets peuvent être retardés, envoyés sporadiquement ou abandonnés. Pour les applications Internet typiques, telles que les e-mails et les transferts de fichiers, une légère dégradation du service est acceptable et, dans de nombreux cas, invisible. Cependant, toute dégradation du service peut affecter négativement les applications nécessitant des délais stricts, telles que la voix et le multimédia.

Définition de DiffServ.

Pour utiliser DiffServ pour QoS, vous devez d'abord définir les catégories suivantes et leurs critères :

1. Classe Créer des classes et définir des critères de classe.
2. Politique Créez des règles, associez des classes à des règles et définissez des instructions de règles.
3. Service Ajouter une stratégie à une interface entrante.

Les paquets sont filtrés, classifiés et traités en fonction de critères définis. Les critères de filtrage et de classification sont définis par une classe. Le traitement est défini par les attributs d'une stratégie. Les attributs de stratégie peuvent être définis par instance de classe, et informatique est ces attributs qui sont appliqués lorsqu'une correspondance se produit. Une règle peut contenir plusieurs classes. Lorsque la stratégie est active, les actions entreprises dépendent de la classe qui correspond au paquet.

Vous commencez la configuration DiffServ en définissant un ou plusieurs critères de correspondance pour une classe. Ensuite, vous configurez une stratégie et ajoutez une ou plusieurs classes à la stratégie. Enfin, vous ajoutez un service, ce qui signifie que vous ajoutez une stratégie à une interface entrante.

Une fois la configuration DiffServ terminée, le commutateur commence le traitement des paquets en testant les critères de correspondance pour un paquet :

- **Tous les types de classe** : L'option All class type spécifie que chaque critère de correspondance au sein d'une classe doit être vrai pour qu'un paquet corresponde à cette classe.
- **Tout type de classe** : L'option type de classe ANY spécifie qu'au moins un critère de correspondance doit être vrai pour qu'un paquet corresponde à cette classe.

Les classes sont testées dans l'ordre dans lequel vous les avez ajoutées à la stratégie. Une stratégie est appliquée à un paquet lorsqu'une correspondance de classe est trouvée dans cette stratégie.

Présentation de l'assistant DiffServ

L'expert DiffServ active DiffServ sur le commutateur en créant une classe de trafic, en ajoutant la classe de trafic à une stratégie, puis en ajoutant la stratégie aux ports et LAG que vous sélectionnez. L'assistant DiffServ effectue les opérations suivantes :

- Crée une classe DiffServ et définit les critères de correspondance utilisés comme filtre pour déterminer si le trafic entrant répond aux exigences pour être membre de la classe.
- Définit les critères de correspondance de classe DiffServ en fonction de la sélection du type de trafic comme suit :
 - **VOIP** : Définit les critères de correspondance pour le trafic VoIP avec le protocole UDP.
 - **HTTP** : Définit les critères de correspondance pour le trafic HTTP vers le port de destination HTTP.
 - **FTP** : Définit les critères de correspondance pour le trafic FTP vers le port FTP de destination.
 - **Telnet** : Définit les critères de correspondance pour le trafic Telnet vers le port Telnet de destination.
 - **Tous les** : Définit les critères de correspondance pour tout le trafic.
- Définit un débit validé pour le type de trafic sélectionné.
- Crée une stratégie Diffserv et ajoute informatique à la classe DiffServ.
- En option, active le contrôle et définit la stratégie Diffserv comme une stratégie simple.

Lorsque le contrôle est activé, le trafic conforme aux critères de correspondance de classe est traité en fonction de la sélection de priorité du trafic sortant, qui gère le trafic conforme comme suit :

- **Elevé(e)** : Mappe la priorité du trafic à la classe DiffServ Expedited Forwarding (EF).
- **Moyen(ne)** : Mappe la priorité du trafic à la classe DiffServ Assured Forwarding (AF31).
- **Faible** : Mappe la priorité du trafic à la classe DiffServ Best effort (BE).

Lorsque le contrôle est désactivé, la priorité sortante (élevée, moyenne ou faible) affecte *tout* le trafic.

- En option, ajoute les ports et LAG sélectionnés à la stratégie.

Utilisez l'assistant DiffServ pour créer une classe de trafic et une stratégie pour une ou plusieurs interfaces

Pour utiliser l'assistant DiffServ afin de créer une classe de trafic et une stratégie pour une ou plusieurs interfaces :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.
Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.
4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **QoS > DiffServ > Assistant DiffServ** .
La page Assistant DiffServ s'affiche.
6. Dans le menu **Traffic type (type de trafic)**, définissez la classe DiffServ en sélectionnant **VoIP, HTTP, FTP, Telnet** ou **tous les**.
7. Dans le champ **débit engagé (Kbps)**, spécifiez le débit en Kbps qui s'applique au trafic de la classe.

La plage va de 1 à la bande passante maximale prise en charge sur l'interface. La valeur par défaut est 1 Kbit/s.

Le taux engagé est appliqué si le contrôle est activé (ce qui est le cas par défaut)

8. Pour désactiver le maintien de l'ordre, décochez la case **maintien de l'ordre**.

Par défaut, le contrôle est activé et la priorité sortante (élevée, moyenne ou faible) est définie comme une stratégie simple. Pour plus d'informations, reportez-vous à l'étape suivante.

Lorsque le contrôle est désactivé, la priorité sortante (élevée, moyenne ou faible) affecte *tout* le trafic.

9. Dans le menu **Outbound Priority**, sélectionnez la priorité du trafic sortant :

- Elevé(e) : Mappe la priorité du trafic à la classe DiffServ Expedited Forwarding (EF).
- Moyen(ne) Mappe la priorité du trafic à la classe DiffServ Assured Forwarding (AF31).
- Faible : Mappe la priorité du trafic à la classe DiffServ Best effort (BE).

Le trafic conforme aux critères de correspondance de classe est traité en fonction de la sélection de priorité sortante.

10. Dans la table ports (ou, si une pile est configurée, dans une ou plusieurs tables ports), cliquez sur chaque port auquel vous souhaitez ajouter la stratégie DiffServ.

Les ports du commutateur (unité 1) sont affichés. Si une pile est configurée, les ports de chaque commutateur empilé (unité 1, unité 2, etc.) sont affichés et vous pouvez sélectionner des ports sur différents commutateurs empilés.

11. Dans la table LAG, cliquez sur chaque LAG auquel vous souhaitez ajouter la stratégie DiffServ.

Tous les LAG sont affichés, qu'une pile soit configurée ou non.

12. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

13. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez le mode DiffServ et affichez les entrées dans les tables MIB privées DiffServ

Vous pouvez activer ou désactiver DiffServ et afficher le nombre actuel et maximal de lignes dans chacune des tables MIB privées DiffServ principales.

Pour configurer le mode DiffServ et afficher les entrées dans les tables MIB privées DiffServ :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **QoS > DiffServ > basique > Configuration DiffServ** .

La page Configuration DiffServ s'affiche.

6. Sélectionnez le mode d'administration de DiffServ :

- Activer. Les services différenciés sont actifs. Il s'agit de l'option par défaut.
- Désactiver : Les services différenciés sont inactifs. Une configuration DiffServ existante est conservée et peut être modifiée mais n'est pas active.

7. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 155 : Informations d'état DiffServ

Champ	Description
Tableau des classes	Nombre de classes DiffServ configurées sur le total autorisé sur le commutateur.
Table de règles de classe	Nombre de règles de classe configurées sur le total autorisé sur le commutateur.
Tableau des règles	Nombre de stratégies configurées sur le total autorisé sur le commutateur.
Table instance de règle	Nombre d'instances de classe de règles configurées sur le total autorisé sur le commutateur.
Tableau attributs de stratégie	Nombre d'attributs de règle configurés (rattachés aux instances de classe de règle) par rapport au total autorisé sur le commutateur.
Tableau des services	Nombre de services configurés (rattachés aux stratégies sur les interfaces spécifiées) par rapport au total autorisé sur le commutateur.

Configurer une classe DiffServ .

Vous pouvez ajouter un nouveau nom de classe DiffServ ou renommer ou supprimer une classe existante. Vous pouvez également définir les critères à associer à une classe DiffServ. Au fur et à mesure que les paquets sont reçus, ces classes DiffServ sont utilisées pour prioriser les paquets. Vous pouvez utiliser plusieurs critères de correspondance dans une classe. La logique est un ET logique booléen pour ce critère.

Ajouter et configurer une classe DiffServ

Vous pouvez ajouter une classe DiffServ et configurer les critères qui doivent être associés à l'informatique.

Pour ajouter et configurer une classe DiffServ :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **QoS > DiffServ > Avancé > Configuration de classe**.

La page Configuration de classe s'affiche.

6. Dans le champ **Service Name** (Nom du service), entrez un nom de service.

Le champ **nom de classe** répertorie également tous les noms de classe DiffServ existants, à partir desquels vous pouvez en sélectionner un pour le modifier ou le supprimer. Le nom de la classe peut contenir entre 1 et 31 caractères alphanumériques.

7. Dans le menu **type de classe**, sélectionnez l'une des options suivantes :

- **Tous:** Tous les critères de correspondance que vous définissez pour la classe doivent être satisfaits pour une correspondance de paquets. Tous signifie le ET logique de tous les critères de correspondance.

Par exemple, si la classe inclut un critère pour une adresse IP et un autre critère pour une adresse MAC, le trafic doit correspondre aux deux critères.

- **Tout:** Tout critère de correspondance que vous définissez pour la classe doit être satisfait pour une correspondance de paquets.

Par exemple, si la classe inclut un critère pour une adresse IP et un autre critère pour une adresse MAC, le trafic doit correspondre à l'un ou l'autre des critères, mais ne doit pas nécessairement correspondre aux deux critères.

Vous ne pouvez sélectionner le type de classe que lorsque vous créez une nouvelle classe. Une fois la classe créée, vous ne pouvez pas modifier le type de classe.

8. Cliquez sur le bouton **Add** (Ajouter).

La nouvelle classe est ajoutée.

9. Après avoir créé la classe, cliquez sur le nom de la classe.

Le nom de la classe est un lien hypertexte vers la page sur laquelle vous pouvez définir la configuration de la classe (voir la figure suivante).

Class Information

Class Name	Class4
Class Type	All

DiffServ Class Configuration

☒ Match Every	Any		
☐ Reference Class			
☐ Class Of Service	0		
☐ VLAN		(1 to 4093)	
☐ Secondary Class of Service	0		
☐ Secondary VLAN		(1 to 4093)	
☐ Ethernet Type	Appletalk		
☐ Source MAC	Address		Mask
☐ Destination MAC	Address		Mask
☐ Protocol Type	ICMP		
☐ Source IP	Address		Mask
☐ Source L4 Port	Domain		(0 to 65535)
☐ Destination IP	Address		Mask
☐ Destination L4 Port	Domain		(0 to 65535)
☐ IP DSCP	af11		
☐ Precedence Value	0	(0 to 7)	
☐ IP ToS	Bit Value		Bit Mask

10. Définissez les critères qui doivent être associés à la classe DiffServ en sélectionnant l'un des boutons radio suivants :

- **Correspondre tous les** : Sélectionnez ce bouton radio pour ajouter une condition de correspondance qui considère que tous les paquets appartiennent à la classe. La seule sélection dans le menu **match Every** est **any**.
- **Classe de référence** : Sélectionnez ce bouton radio pour référencer une autre classe pour les critères. Les critères de correspondance définis dans la classe de référence fonctionnent comme critères de correspondance en plus des critères de correspondance que vous définissez pour la classe sélectionnée. Après avoir sélectionné le bouton radio, les classes qui peuvent être référencées sont affichées. Sélectionnez la classe à référencer. Une classe ne peut référencer qu'une autre classe du même type.
- **Classe de service** : Sélectionnez ce bouton radio pour exiger que la valeur de classe de service (cos) dans un en-tête de trame Ethernet corresponde à la valeur de classe de service spécifiée. Cette option répertorie toutes les valeurs pour le critère de correspondance de classe de service dans la plage 0 à 7 dans laquelle vous pouvez en sélectionner une.
- **VLAN** : Sélectionnez ce bouton radio pour exiger que l'ID VLAN d'un paquet corresponde à un ID VLAN. L'ID VLAN peut être compris entre 1 et 4093.

- **Classe de service secondaire** : Sélectionnez ce bouton radio pour exiger que la valeur de classe de service (cos) secondaire dans un en-tête de trame Ethernet corresponde à la valeur de classe de service secondaire spécifiée.
- **VLAN secondaire** : Sélectionnez ce bouton radio pour exiger que l'ID VLAN d'un paquet corresponde à un ID VLAN secondaire. L'ID VLAN peut être compris entre 1 et 4093.
- **Type Ethernet** : Sélectionnez ce bouton radio pour exiger que la valeur EtherType de l'en-tête de trame Ethernet corresponde à la valeur EtherType spécifiée. Après avoir sélectionné le bouton radio, sélectionnez le mot-clé EtherType dans le menu des protocoles courants mappés à leur valeur EtherType. Vous pouvez également sélectionner **valeur utilisateur** dans le menu et entrer une valeur dans la plage hexadécimale de 600 à ffff.
- **Source MAC** (Adresse IP source). Sélectionnez ce bouton radio pour exiger que l'adresse MAC source d'un paquet corresponde à l'adresse MAC spécifiée. Après avoir sélectionné ce bouton radio, utilisez les champs suivants pour configurer les critères de correspondance de l'adresse MAC source :
 - **Address** (Adresse). Adresse MAC source à faire correspondre. L'adresse MAC source est spécifiée sous forme de six nombres hexadécimaux à deux chiffres séparés par deux-points.
 - **Masque** Le masque MAC, qui spécifie les bits de l'adresse MAC source à comparer avec la trame Ethernet. Utilisez FS et zéros pour configurer le masque MAC. Un F signifie que le bit est vérifié, et un zéro dans une position de bit signifie que les données ne sont pas significatives. Par exemple, si l'adresse MAC est aa:bb:cc:dd :EE:ff et que le masque est ff:ff :00 :00 :00 :00, toutes les adresses MAC avec aa:bb:xx:xx:xx:xx résultent en une correspondance (où x est un nombre hexadécimal). Notez qu'il ne s'agit pas d'un masque générique utilisé par les listes de contrôle d'accès.
- **MAC de destination** : Sélectionnez ce bouton radio pour exiger que l'adresse MAC de destination d'un paquet corresponde à l'adresse MAC spécifiée. Après avoir sélectionné le bouton radio, utilisez les champs suivants pour configurer les critères de correspondance de l'adresse MAC de destination :
 - **Address** (Adresse). Adresse MAC de destination à laquelle correspondre. L'adresse MAC de destination est spécifiée sous la forme de six nombres hexadécimaux à deux chiffres séparés par deux-points.
 - **Masque** Spécifiez le masque d'adresse MAC de destination, qui représente les bits de l'adresse MAC de destination à comparer à une trame Ethernet. Utilisez FS et zéros pour configurer le masque MAC. Un F signifie que le bit est vérifié, et un zéro dans une position de bit signifie que les données ne sont pas significatives. Par exemple, si l'adresse MAC est aa:bb:cc:dd :EE:ff et que le masque est ff:ff :00 :00 :00 :00, toutes les adresses MAC avec

aa:bb:xx:xx:xx:xx résultent en une correspondance (où x est un nombre hexadécimal). Notez qu'il ne s'agit pas d'un masque générique utilisé par les listes de contrôle d'accès.

- **Type de protocole** : Sélectionnez ce bouton radio pour exiger que le protocole de couche 4 d'un paquet corresponde au protocole spécifié, que vous devez sélectionner dans le menu. Vous pouvez également sélectionner **autre** dans le menu et entrer un numéro de protocole compris entre 0 et 255.
- **Source IP** (Adresse IP source). Sélectionnez ce bouton radio pour exiger que l'adresse IP source d'un paquet corresponde à l'adresse IP spécifiée. Après avoir sélectionné le bouton radio, utilisez les champs suivants pour configurer les critères de correspondance de l'adresse IP source :
 - **Address** (Adresse). Format de l'adresse IP source à faire correspondre en virgule décimale.
 - Masque Masque binaire au format décimal à points IP indiquant les parties de l'adresse IP source à utiliser pour la correspondance avec le contenu du paquet.
- **Port source L4** : Sélectionnez ce bouton radio pour exiger que le port source TCP/UDP d'un paquet corresponde au protocole spécifié, que vous devez sélectionner dans le menu. Vous pouvez également sélectionner **autre** dans le menu et entrer un numéro de port compris entre 0 et 65535.
- **IP destination** Sélectionnez ce bouton radio pour exiger que l'adresse IP de destination d'un paquet corresponde à l'adresse IP spécifiée. Après avoir sélectionné le bouton radio, utilisez les champs suivants pour configurer les critères de correspondance de l'adresse IP de destination :
 - **Address** (Adresse). Format de l'adresse IP de destination à faire correspondre en décimales à points.
 - Masque Masque binaire au format décimal à points IP indiquant les parties de l'adresse IP de destination à utiliser pour la correspondance avec le contenu du paquet.
- **Port L4 de destination** : Sélectionnez ce bouton radio pour exiger que le port de destination TCP/UDP d'un paquet corresponde au protocole spécifié. Vous pouvez également sélectionner **autre** dans le menu et entrer un numéro de port compris entre 0 et 65535.
- **IP DSCP** : Sélectionnez ce bouton radio pour exiger que la valeur DSCP (IP DiffServ Code point) du paquet corresponde au code de mot clé DSCP IP spécifié, que vous devez sélectionner dans le menu. Vous pouvez également sélectionner **autre** dans le menu et entrer une valeur DSCP IP comprise entre 0 et 63. La valeur DSCP est définie comme les 6 bits de poids fort de l'octet de type de service dans l'en-tête IP.

- **Valeur de priorité** : Sélectionnez ce bouton radio pour que la valeur de priorité IP du paquet corresponde au nombre spécifié de 0 à 7, que vous devez sélectionner dans le menu. Le champ IP Precedence dans un paquet est défini comme les 3 bits de poids fort de l'octet de type de service dans l'en-tête IP.
- **IP ToS** : Sélectionnez ce bouton radio pour exiger que les bits de type de service (ToS) du paquet dans l'en-tête IP correspondent à la valeur spécifiée. Le champ IP ToS dans un paquet est défini comme les 8 bits de l'octet de type de service dans l'en-tête IP. Après avoir sélectionné le bouton radio, utilisez les champs suivants pour configurer les critères de correspondance ToS :
 - **Valeur de bit** : Entrez une valeur d'octet hexadécimal à deux chiffres comprise entre 00 et ff pour correspondre aux bits du champ ToS d'un paquet.
 - **Masque de bit** : Spécifiez les positions de bits utilisées pour la comparaison avec le champ IP ToS dans un paquet.

11. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

12. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la section Résumé de la classe.

Table 156 : Configuration de classe DiffServ, informations de synthèse de classe

Champ	Description
Critères de correspondance	Critères de correspondance configurés pour la classe spécifiée.
Valeurs	Les valeurs des critères de correspondance configurés.

Renommer une classe DiffServ existante

Vous pouvez modifier le nom d'une classe DiffServ existante.

Pour renommer une classe DiffServ existante :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
 Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
 La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
 La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **QoS > DiffServ > Avancé > Configuration de classe**.

La page Configuration de classe s'affiche.

6. Cochez la case en regard du nom de la classe.

7. Dans le champ **nom de classe**, spécifiez le nouveau nom.

8. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Modifiez les critères d'une classe DiffServ existante

Vous pouvez modifier les critères d'une classe DiffServ existante.

Pour modifier les critères d'une classe DiffServ existante :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **QoS > DiffServ > Avancé > Configuration de classe**.

La page Configuration de classe s'affiche.

6. Cliquez sur le nom de la classe, qui est un lien hypertexte.

La page sur laquelle vous pouvez modifier la configuration de la classe s'affiche.

7. Modifiez la configuration de la classe si nécessaire.

8. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimer une classe DiffServ

Vous pouvez supprimer une classe DiffServ existante dont vous n'avez plus besoin.

Pour supprimer une classe DiffServ :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **QoS > DiffServ > Avancé > Configuration de classe**.

La page Configuration de classe s'affiche.

6. Cochez la case en regard du nom de la classe.

7. Cliquez sur le bouton **Supprimer**.

La classe est supprimée.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez une classe IPv6 DiffServ

Le commutateur prend en charge la liste de contrôle d'accès QoS et la fonctionnalité DiffServ pour IPv6 en prenant en charge la classification des paquets IPv6. Une liste de contrôle d'accès IPv6 a le même but qu'une liste de contrôle d'accès IPv4.

Un paquet IPv6 Ethernet se distingue d'un paquet IPv4 par sa valeur Ethertype unique, de sorte que tous les classificateurs IPv6 incluent le champ Ethertype, même si vous ne pouvez pas configurer sa valeur pour une classe IPv6 sur le commutateur.

Les adresses IPv6 de destination et source utilisent une valeur de longueur de préfixe au lieu d'un masque individuel pour les qualifier d'adresses de sous-réseau ou d'adresses d'hôte. Les paquets qui correspondent à un classificateur IPv6 peuvent être marqués avec le champ IP DSCP dans l'octet de classe de trafic.

Vous pouvez également affecter une liste de contrôle d'accès IPv6 avec des interfaces lagger d'affectation DiffServ.

Vous pouvez ajouter un nouveau nom de classe DiffServ ou renommer ou supprimer une classe existante. Au fur et à mesure que les paquets sont reçus, ces classes DiffServ sont utilisées pour prioriser les paquets. Vous pouvez utiliser plusieurs critères de correspondance dans une classe. La logique est un ET logique booléen pour ce critère.

Ajoutez et configurez une classe IPv6 DiffServ

Vous pouvez ajouter une classe IPv6 DiffServ et configurer les critères qui doivent être associés à informatique.

Pour configurer une classe IPv6 DiffServ :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **QoS > DiffServ > Avancé > Configuration de classe IPv6** .

La page Configuration de classe s'affiche.

6. Dans le champ **Service Name** (Nom du service), entrez un nom de service.

Le champ **nom de classe** répertorie également tous les noms de classe DiffServ existants, à partir desquels vous pouvez en sélectionner un pour le modifier ou le supprimer. Le nom de la classe peut contenir entre 1 et 31 caractères alphanumériques.

7. Dans le menu **type de classe**, sélectionnez l'une des options suivantes :

- **Tous:** Tous les critères de correspondance que vous définissez pour la classe doivent être satisfaits pour une correspondance de paquets. Tous signifie le ET logique de tous les critères de correspondance.

Par exemple, si la classe inclut un critère pour une adresse IP et un autre critère pour une adresse MAC, le trafic doit correspondre aux deux critères.

- **Tout:** Tout critère de correspondance que vous définissez pour la classe doit être satisfait pour une correspondance de paquets.

Par exemple, si la classe inclut un critère pour une adresse IP et un autre critère pour une adresse MAC, le trafic doit correspondre à l'un ou l'autre des critères, mais ne doit pas nécessairement correspondre aux deux critères.

Vous ne pouvez sélectionner le type de classe que lorsque vous créez une nouvelle classe. Une fois la classe créée, vous ne pouvez pas modifier le type de classe.

8. Cliquez sur le bouton **Add** (Ajouter).

La nouvelle classe est ajoutée.

9. Après avoir créé la classe, cliquez sur le nom de la classe.

Le nom de la classe est un lien hypertexte vers la page sur laquelle vous pouvez définir la configuration de la classe (voir la figure suivante).

IPv6 Class Information

Class Name	Class1
Class Type	All

IPv6 DiffServ Class Configuration

☒ Match Every	Any	
☐ Reference Class	Class4	
☐ Protocol Type	ICMPv6	(0 to 255)
☐ Source Prefix/Length		
☐ Source L4 Port	Domain	(0 to 65535)
☐ Destination Prefix/Length		
☐ Destination L4 Port	Domain	(0 to 65535)
☐ Flow Label	(0 to 1048575)	
☐ IP DSCP	af11	(0 to 63)

10. Définissez les critères à associer à une classe DiffServ :

- **Correspondre tous les** : Sélectionnez ce bouton radio pour ajouter une condition de correspondance qui considère que tous les paquets appartiennent à la classe. La seule sélection dans le menu **match Every** est **any**.
- **Classe de référence** : Sélectionnez ce bouton radio pour référencer une autre classe pour les critères. Les critères de correspondance définis dans la classe de référence fonctionnent comme critères de correspondance en plus des critères de correspondance que vous définissez pour la classe sélectionnée. Après avoir sélectionné cette option, les classes qui peuvent être référencées sont affichées. Sélectionnez la classe à référencer. Une classe peut référencer une autre classe du même type.
- **Type de protocole** : Sélectionnez ce bouton radio pour exiger que le protocole de couche 4 d'un paquet corresponde au protocole spécifié, que vous devez sélectionner dans le menu. Le menu inclut **autre** comme sélection, ce qui vous permet de saisir un numéro de protocole compris entre 0 et 255.
- **Longueur du préfixe source** : Sélectionnez ce bouton radio pour exiger que le préfixe source et la longueur de préfixe d'un paquet correspondent au préfixe source IPv6 et à la longueur de préfixe spécifiée. Le préfixe doit toujours être spécifié avec la longueur du préfixe. Le préfixe peut être compris entre 0 et FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF et la longueur du préfixe peut être comprise entre 0 et 128.
- **Port source L4** : Sélectionnez ce bouton radio pour exiger que le port source TCP/UDP d'un paquet corresponde au protocole spécifié, que vous devez sélectionner dans le menu. La plage est comprise entre 0 et 65535. Le menu inclut **autre** comme option pour les ports sans nom.
- **Longueur du préfixe de destination** : Sélectionnez ce bouton radio pour exiger que le préfixe de destination et la longueur de préfixe d'un paquet correspondent au préfixe et à la longueur de préfixe IPv6 source spécifiés. Le préfixe doit toujours être spécifié avec la longueur du préfixe. Le préfixe peut être compris entre 0 et FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF et la longueur du préfixe peut être comprise entre 0 et 128.
- **Port L4 de destination** : Sélectionnez ce bouton radio pour exiger que le port de destination TCP/UDP d'un paquet corresponde au protocole spécifié, que vous devez sélectionner dans le menu. La plage est comprise entre 0 et 65535. Le menu inclut **autre** comme option pour les ports sans nom.
- **Étiquette de flux** : Sélectionnez ce bouton radio pour exiger que l'étiquette de flux d'un paquet corresponde à l'étiquette de flux spécifiée. L'étiquette de flux est un numéro de 20 bits unique à un paquet IPv6 et utilisé par les stations terminales pour indiquer la gestion QoS dans les routeurs. Le libellé de flux peut être spécifié dans la plage de 0 à 1048575.
- **IP DSCP** : Sélectionnez ce bouton radio pour exiger que la valeur DSCP (IP DiffServ Code point) du paquet corresponde au code de mot clé DSCP IP spécifié,

que vous devez sélectionner dans le menu. Le menu inclut **autre** comme sélection, ce qui vous permet de saisir une valeur DSCP IP comprise entre 0 et 63. La valeur DSCP est définie comme les 6 bits de poids fort de l'octet de type de service dans l'en-tête IP.

11. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

12. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les informations en lecture seule affichées dans la section Résumé de la classe.

Table 157 : Résumé de la classe de configuration de la classe IPv6 DiffServ

Champ	Description
Critères de correspondance	Critères de correspondance configurés pour la classe spécifiée.
Valeurs	Les valeurs des critères de correspondance configurés.

Renommez une classe IPv6 DiffServ existante

Vous pouvez modifier le nom d'une classe IPv6 DiffServ existante.

Pour renommer une classe IPv6 DiffServ existante :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **QoS > DiffServ > Avancé > Configuration de classe IPv6**.

La page Configuration de classe s'affiche.

6. Cochez la case en regard du nom de la classe.

7. Dans le champ **nom de classe**, spécifiez le nouveau nom.

8. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Modifiez les critères d'une classe IPv6 DiffServ existante

Vous pouvez modifier les critères d'une classe IPv6 DiffServ existante.

Pour modifier les critères d'une classe IPv6 DiffServ existante :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **QoS > DiffServ > Avancé > Configuration de classe IPv6**.

La page Configuration de classe s'affiche.

6. Cliquez sur le nom de la classe, qui est un lien hypertexte.

La page sur laquelle vous pouvez modifier la configuration de la classe s'affiche.

7. Modifiez la configuration de la classe si nécessaire.

8. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimez une classe IPv6 DiffServ

Vous pouvez supprimer une classe IPv6 DiffServ dont vous n'avez plus besoin.

Pour supprimer une classe IPv6 DiffServ :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **QoS > DiffServ > Avancé > Configuration de classe IPv6**.

La page Configuration de classe s'affiche.

6. Cochez la case en regard du nom de la classe.

7. Cliquez sur le bouton **Supprimer**.

La classe est supprimée.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurer une stratégie DiffServ.

Vous pouvez associer un ensemble de classes à une ou plusieurs stratégies.

Ajouter et configurer une stratégie DiffServ

Vous pouvez ajouter une stratégie, configurer le type de stratégie, ajouter une classe de membre à la stratégie, puis configurer les attributs de stratégie.

Pour ajouter et configurer une stratégie DiffServ :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.
4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **QoS > DiffServ > Avancé > Configuration des stratégies** .
La page Configuration de la stratégie s'affiche.
6. Dans le champ **Service Name** (Nom du service), entrez un nom de service.
Le nom de la classe de stratégie peut contenir entre 1 et 31 caractères alphanumériques.
7. Dans le menu **Policy type**, sélectionnez la direction du flux de trafic à laquelle la stratégie doit être appliquée :
 - **po**. La stratégie est appliquée au trafic entrant.
 - **Sortie**: La stratégie est appliquée au trafic sortant.
8. Dans le menu **classe membre**, sélectionnez une classe existante que vous souhaitez associer à la nouvelle stratégie.
9. Cliquez sur le bouton **Add** (Ajouter).
La nouvelle stratégie est ajoutée.
10. Après avoir créé la stratégie, cliquez sur son nom.
Le nom de la stratégie est un lien hypertexte.
La page qui s'affiche vous permet de définir les attributs de stratégie.
11. Configurez les attributs de stratégie en sélectionnant *l'un* des boutons radio suivants :
 - **Attribuer une file d'attente** : Sélectionnez ce bouton radio pour spécifier que le trafic doit être affecté à une file d'attente, que vous devez sélectionner dans

le menu. La file d'attente est exprimée sous la forme d'une valeur comprise entre 0 et 7.

- **Abandonné** Sélectionnez ce bouton radio pour exiger que chaque paquet soit abandonné.
- **Mark VLAN cos** : Sélectionnez ce bouton radio pour spécifier la priorité VLAN, que vous devez sélectionner dans le menu. La priorité VLAN est exprimée sous la forme d'une valeur comprise entre 0 et 7.
- **Marquer la priorité IP** : Sélectionnez ce bouton radio pour exiger que les paquets soient marqués avec une valeur de priorité IP avant d'être transférés. Vous devez sélectionner une valeur de priorité IP comprise entre 0 et 7 dans le menu.
- **Miroir** Sélectionnez ce bouton radio pour exiger que les paquets soient mis en miroir sur une interface ou un lag, dont vous devez sélectionner un dans le menu.
- **Redirection...** Sélectionnez ce bouton radio pour exiger que les paquets soient redirigés vers une interface ou un lag, dont vous devez sélectionner un dans le menu.
- **Mark IP DSCP** : Sélectionnez ce bouton radio pour que le paquet soit marqué avec un code de mot clé IP DSCP, que vous devez sélectionner dans le menu. La valeur DSCP est définie comme les 6 bits de poids fort de l'octet de type de service dans l'en-tête IP.
- **Politique simple** : Sélectionnez ce bouton radio pour définir que les paquets correspondants sont traités par une stratégie de trafic simple, qui est daltonique et pour laquelle les classes de couleurs ne s'appliquent pas.

Une stratégie simple prend en charge un débit de données unique et entraîne une action pour les paquets conformes à la stratégie et une action pour les paquets qui violent la stratégie. Vous pouvez configurer l'action pour les paquets conformes à la stratégie, mais l'action pour les paquets qui violent la stratégie est toujours DROP, c'est-à-dire que ces paquets sont toujours abandonnés.

- a. Spécifiez le débit de trafic et la taille de buste pour les paquets conformes à la stratégie simple.
 - **Taux engagé** . Dans le menu, sélectionnez **pourcentage** ou **Kbps**, puis spécifiez le débit validé appliqué aux paquets conformes en entrant une valeur comprise entre 1 et 100 % ou entre 1 et 4294967295 kilobits par seconde (Kbps). Le taux engagé est utilisé pour limiter le taux d'arrivée du trafic conforme.
 - **Taille de rafale engagée** . Spécifiez la taille de rafale appliquée aux paquets conformes en entrant une valeur comprise entre 1 et 128 Ko (Ko). La taille de rafale validée est utilisée pour limiter la quantité de trafic conforme.
- b. **Confirmer l'action** : Spécifiez une action de stratégie pour les paquets conformes à la stratégie simple.

- Envoyer Les paquets sont transmis sans modification. Il s'agit de l'action de confirmation par défaut.
 - Abandonné Les paquets sont abandonnés.
 - **Mark cos** : Les paquets sont marqués par DiffServ avec la valeur cos spécifiée avant d'être transférés. Cette sélection nécessite que le champ marquer cos soit défini. Vous devez sélectionner une valeur cos comprise entre 0 et 7 dans le menu.
 - **Marquer la priorité IP** : Ces paquets sont marqués par DiffServ avec la valeur IP Precedence spécifiée avant d'être transférés. Cette sélection nécessite que le champ marquer la priorité IP soit défini. Vous devez sélectionner une valeur de priorité IP comprise entre 0 et 7 dans le menu.
 - **Mark IP DSCP** : Les paquets sont marqués par DiffServ avec la valeur DSCP spécifiée avant d'être transférés. Cette sélection nécessite que le champ DSCP soit défini. Vous devez sélectionner un code DSCP dans le menu ou saisir une valeur DSCP IP comprise entre 0 et 63 dans le champ situé à côté du menu. Une valeur que vous entrez dans le champ remplace toute sélection du menu. La valeur DSCP est définie comme les six bits de poids fort de l'octet de type de service dans l'en-tête IP.
- c. **Action violer** : Spécifiez une action de stratégie pour les paquets qui enfreignent la stratégie simple.
- Envoyer Les paquets sont transmis sans modification. Il s'agit de l'action de violation par défaut.
 - Abandonné Les paquets sont abandonnés.
 - **Mark cos** : Les paquets sont marqués par DiffServ avec la valeur cos spécifiée avant d'être transférés. Cette sélection nécessite que le champ marquer cos soit défini. Vous devez sélectionner une valeur cos comprise entre 0 et 7 dans le menu.
 - **Marquer la priorité IP** : Ces paquets sont marqués par DiffServ avec la valeur IP Precedence spécifiée avant d'être transférés. Cette sélection nécessite que le champ marquer la priorité IP soit défini. Vous devez sélectionner une valeur de priorité IP comprise entre 0 et 7 dans le menu.
 - **Mark IP DSCP** : Les paquets sont marqués par DiffServ avec la valeur DSCP spécifiée avant d'être transférés. Cette sélection nécessite que le champ DSCP soit défini. Vous devez sélectionner un code DSCP dans le menu ou saisir une valeur DSCP IP comprise entre 0 et 63 dans le champ situé à côté du menu. Une valeur que vous entrez dans le champ remplace toute sélection du menu. La valeur DSCP est définie comme les six bits de poids fort de l'octet de type de service dans l'en-tête IP.
- **Deux taux** : Sélectionnez ce bouton radio pour définir un style de contrôle du trafic à deux débits pour la classe. Une politique à deux taux diffère d'une

politique simple en ce sens qu'elle vous permet de définir un taux de crête et une taille de rafale de crête, en plus du taux engagé et de la taille de rafale engagée.

Une stratégie à deux débits prend en charge deux débits de données et entraîne une action et pour les paquets conformes à la stratégie et une action pour les paquets qui violent la stratégie.

Par défaut, la police à deux taux est daltonique et les classes de couleurs ne s'appliquent pas.

- a. Spécifiez les débits de trafic et les tailles de buste pour les paquets conformes à la stratégie à deux débits.
 - **Taux engagé** : Dans le menu, sélectionnez **pourcentage** ou **Kbps**, puis spécifiez le débit validé appliqué aux paquets conformes en entrant une valeur comprise entre 1 et 100 % ou entre 1 et 4294967295 kilobits par seconde (Kbps). Le débit engagé est utilisé pour garantir la bande passante autorisée du trafic conforme.
 - **Taille de rafale validée** : Spécifiez la taille de rafale appliquée aux paquets conformes en entrant une valeur comprise entre 1 et 128 Ko (Ko). La taille de rafale validée est utilisée pour limiter le nombre maximal d'octets dans une rafale (instance très courte) de trafic conforme.
 - **Taux de pointe** : Spécifiez le débit maximal appliqué aux paquets conformes en entrant une valeur comprise entre 1 et 4294967295 kilobits par seconde (Kbit/s). Le débit de pointe est utilisé pour limiter la quantité de trafic conforme pouvant dépasser le débit engagé.
 - **Taille de rafale de crête** : Spécifiez la taille de rafale maximale appliquée aux paquets conformes en entrant une valeur comprise entre 1 et 128 Ko (Ko). La taille de rafale de crête est utilisée pour limiter la quantité de trafic conforme pouvant dépasser le débit de crête.
- b. **Action de conformité** : Spécifiez une action de stratégie pour les paquets conformes à la stratégie à deux débits.
 - Envoyer Les paquets sont transmis sans modification. Il s'agit de l'action de confirmation par défaut.
 - Abandonné Les paquets sont abandonnés.
 - **Mark cos** : Les paquets sont marqués par DiffServ avec la valeur cos spécifiée avant d'être transférés. Cette sélection nécessite que le champ marquer cos soit défini. Vous devez sélectionner une valeur cos comprise entre 0 et 7 dans le menu.
 - **Marquer la priorité IP** : Ces paquets sont marqués par DiffServ avec la valeur IP Precedence spécifiée avant d'être transférés. Cette sélection

nécessite que le champ marquer la priorité IP soit défini. Vous devez sélectionner une valeur de priorité IP comprise entre 0 et 7 dans le menu.

- **Mark IP DSCP** : Les paquets sont marqués par DiffServ avec la valeur DSCP spécifiée avant d'être transférés. Cette sélection nécessite que le champ DSCP soit défini. Vous devez sélectionner un code DSCP dans le menu ou saisir une valeur DSCP IP comprise entre 0 et 63 dans le champ situé à côté du menu. Une valeur que vous entrez dans le champ remplace toute sélection du menu.

La valeur DSCP est définie comme les six bits de poids fort de l'octet de type de service dans l'en-tête IP.

- c. **Dépasser l'action** : Spécifiez une action de stratégie pour les paquets qui dépassent la stratégie à deux débits.
 - Envoyer Les paquets sont transmis sans modification. Il s'agit de l'action de violation par défaut.
 - Abandonné Les paquets sont abandonnés.
 - **Mark cos** : Les paquets sont marqués par DiffServ avec la valeur cos spécifiée avant d'être transférés. Cette sélection nécessite que le champ marquer cos soit défini. Vous devez sélectionner une valeur cos comprise entre 0 et 7 dans le menu.
 - **Marquer la priorité IP** : Ces paquets sont marqués par DiffServ avec la valeur IP Precedence spécifiée avant d'être transférés. Cette sélection nécessite que le champ marquer la priorité IP soit défini. Vous devez sélectionner une valeur de priorité IP comprise entre 0 et 7 dans le menu.
 - **Mark IP DSCP** : Les paquets sont marqués par DiffServ avec la valeur DSCP spécifiée avant d'être transférés. Cette sélection nécessite que le champ DSCP soit défini. Vous devez sélectionner un code DSCP dans le menu ou saisir une valeur DSCP IP comprise entre 0 et 63 dans le champ situé à côté du menu. Une valeur que vous entrez dans le champ remplace toute sélection du menu.

La valeur DSCP est définie comme les six bits de poids fort de l'octet de type de service dans l'en-tête IP.

- d. **Action violer** : Spécifiez une action de stratégie pour les paquets qui enfreignent la stratégie à deux débits.
 - Envoyer Les paquets sont transmis sans modification. Il s'agit de l'action de violation par défaut.
 - Abandonné Les paquets sont abandonnés.
 - **Mark cos** : Les paquets sont marqués par DiffServ avec la valeur cos spécifiée avant d'être transférés. Cette sélection nécessite que le champ marquer cos soit défini. Vous devez sélectionner une valeur cos comprise entre 0 et 7 dans le menu.

- **Marquer la priorité IP** : Ces paquets sont marqués par DiffServ avec la valeur IP Precedence spécifiée avant d'être transférés. Cette sélection nécessite que le champ marquer la priorité IP soit défini. Vous devez sélectionner une valeur de priorité IP comprise entre 0 et 7 dans le menu.
- **Mark IP DSCP** : Les paquets sont marqués par DiffServ avec la valeur DSCP spécifiée avant d'être transférés. Cette sélection nécessite que le champ DSCP soit défini. Vous devez sélectionner un code DSCP dans le menu ou saisir une valeur DSCP IP comprise entre 0 et 63 dans le champ situé à côté du menu. Une valeur que vous entrez dans le champ remplace toute sélection du menu.

La valeur DSCP est définie comme les six bits de poids fort de l'octet de type de service dans l'en-tête IP.

12. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

13. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 158 : Configuration de stratégie DiffServ, attributs de stratégie

Champ	Description
Nom de la politique	Nom de la stratégie DiffServ
Type de police	Le type de la police (entrée ou sortie)
Nom de la classe membre	Instances de classe associées dans la stratégie

Renommer une stratégie DiffServ existante

Vous pouvez modifier le nom d'une stratégie DiffServ existante.

Pour renommer une stratégie DiffServ existante :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **QoS > DiffServ > Avancé > Configuration des stratégies**.

La page Configuration de la stratégie s'affiche.

6. Cochez la case en regard du nom de la stratégie.
7. Dans le champ **Policy Name**, spécifiez le nouveau nom.
8. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Modifiez les attributs d'une stratégie DiffServ existante

Vous pouvez modifier les attributs d'une stratégie DiffServ existante.

Pour modifier les attributs d'une stratégie DiffServ existante :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **QoS > DiffServ > Avancé > Configuration des stratégies**.

La page Configuration de la stratégie s'affiche.

6. Cliquez sur le nom de la stratégie, qui est un lien hypertexte.

La page sur laquelle vous pouvez modifier les attributs de stratégie s'affiche.

7. Modifiez les attributs de la règle si nécessaire.

8. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Modifier ou supprimer une classe d'une stratégie DiffServ existante

Vous pouvez modifier une classe dans une stratégie DiffServ existante ou supprimer une classe de la stratégie.

Pour modifier ou supprimer une classe d'une stratégie DiffServ existante :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.
4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **QoS > DiffServ > Avancé > Configuration des stratégies** .
La page Configuration de la stratégie s'affiche.
6. Cochez la case en regard du nom de la stratégie.
7. Effectuez l'une des opérations suivantes :
 - Pour modifier la classe, sélectionnez une autre classe dans le menu **classe membre**.
 - Pour supprimer la classe, sélectionnez **aucun** dans le menu **classe membre**.
8. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimer une stratégie DiffServ

Vous pouvez supprimer une stratégie DiffServ dont vous n'avez plus besoin.

Pour supprimer une stratégie DiffServ :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **QoS > DiffServ > Avancé > Configuration des stratégies**.

La page Configuration de la stratégie s'affiche.

6. Cochez la case en regard du nom de la stratégie.

7. Cliquez sur le bouton **Supprimer**.

La stratégie est supprimée.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez l'interface de service DiffServ .

Vous pouvez attribuer (joindre) une stratégie entrante et une stratégie sortante à une interface.

Attachez des stratégies DiffServ à une interface

Vous pouvez associer une stratégie entrante, une stratégie sortante ou les deux types de stratégies à une interface.

Pour associer des stratégies DiffServ à une interface :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **QoS > DiffServ > Avancé > Configuration de l'interface de service**.

La page Configuration de l'interface de service s'affiche.

6. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :

- **1 ou ID d'unité pour un commutateur empilé :**

- 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
 - **ID d'unité pour un commutateur empilé** : Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
 - LAG Seuls les LAG sont affichés.
 - **Tous**: Les interfaces physiques et les LAG sont affichés, ou pour une pile de commutateurs, les interfaces physiques de tous les commutateurs de la pile et les LAG sont affichés.
7. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :
- Pour afficher ou effacer les statistiques d'une seule interface, cochez la case associée à l'interface ou saisissez le numéro de l'interface dans le champ **aller à l'interface** et cliquez sur le bouton **aller**.
 - Pour configurer plusieurs interfaces avec les mêmes paramètres, cochez la case associée à chaque interface.
 - Pour configurer toutes les interfaces avec les mêmes paramètres, cochez la case dans la ligne d'en-tête.
8. Dans le menu **Policy in Name**, sélectionnez le nom d'une stratégie pour le trafic entrant.
9. Dans le menu **Policy Out Name**, sélectionnez le nom d'une stratégie pour le trafic sortant.
10. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
11. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 159 : Informations sur la configuration de l'interface de service

Champ	Description
Direction	Direction du trafic (entrée, sortie ou entrée et sortie) de la ou des stratégies sur l'interface de service.
Statut opérationnel	L'état opérationnel de cette interface de service (haut ou bas). L'état opérationnel est affiché comme UP si toutes les conditions suivantes sont remplies : • La classe attachée est valide et inclut au moins une règle correspondante. • La stratégie associée est valide et inclut au moins un attribut. • Le port est activé, c'est-à-dire que la liaison physique du port est à l'état <i>actif</i>.

Modifiez une ou les deux stratégies DiffServ pour une interface

Vous pouvez modifier la stratégie de trafic entrant, la stratégie de trafic sortant ou les deux pour une interface.

Pour modifier une ou les deux stratégies DiffServ pour une interface :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **QoS > DiffServ > Avancé > Configuration de l'interface de service**

.

La page Configuration de l'interface de service s'affiche.

6. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :

- **1 ou ID d'unité pour un commutateur empilé :**

- 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
 - **ID d'unité pour un commutateur empilé** : Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
 - LAG Seuls les LAG sont affichés.
 - **Tous**: Les interfaces physiques et les LAG sont affichés, ou pour une pile de commutateurs, les interfaces physiques de tous les commutateurs de la pile et les LAG sont affichés.
7. Cochez la case associée à l'interface ou saisissez le numéro de l'interface dans le champ **aller à l'interface** et cliquez sur le bouton **aller**
 8. Pour sélectionner une autre stratégie entrante, dans le menu **Policy in Name**, sélectionnez un autre nom de stratégie.
 9. Pour sélectionner une autre stratégie sortante, sélectionnez un autre nom de stratégie dans le menu **Policy Out Name**.
 10. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
 11. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimez une ou les deux stratégies DiffServ d'une interface

Vous pouvez supprimer la stratégie entrante, la stratégie sortante ou les deux d'une interface.

Pour supprimer une ou les deux stratégies DiffServ d'une interface :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **QoS > DiffServ > Avancé > Configuration de l'interface de service**

.

La page Configuration de l'interface de service s'affiche.

6. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :

- **1 ou ID d'unité pour un commutateur empilé :**
 - 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
 - **ID d'unité pour un commutateur empilé :** Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
- **LAG** Seuls les LAG sont affichés.
- **Tous:** Les interfaces physiques et les LAG sont affichés, ou pour une pile de commutateurs, les interfaces physiques de tous les commutateurs de la pile et les LAG sont affichés.

7. Cochez la case associée à l'interface ou saisissez le numéro de l'interface dans le champ **aller à l'interface** et cliquez sur le bouton **aller**
8. Pour supprimer la stratégie de trafic entrant, dans le menu **Policy in Name**, sélectionnez None.
9. Pour supprimer la stratégie sortante, dans le menu **Policy Out Name**, sélectionnez aucun.
10. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
11. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Afficher les statistiques du service DiffServ

Vous pouvez afficher des informations statistiques de niveau de service sur toutes les interfaces auxquelles les stratégies DiffServ sont associées.

Pour afficher les statistiques du service DiffServ :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **QoS > DiffServ > Avancé > statistiques de service**.

La page statistiques de service s'affiche.

6. Utilisez le menu **Rechercher** pour rechercher des statistiques DiffServ par interface ou classe de membre :

- Pour effectuer une recherche par interface, sélectionnez **interface**, entrez l'interface au format unité/emplacement/port (par exemple, 1/0/13), puis cliquez sur le bouton **aller**.

Si l'entrée existe, l'entrée est affichée en tant que première entrée, suivie des entrées restantes.

- Pour effectuer une recherche par classe de membre, sélectionnez **classe de membre**, entrez la classe de membre et cliquez sur le bouton **aller**.

Si une entrée avec une classe de membre correspondante existe, l'entrée est affichée en tant que première entrée, suivie des entrées restantes. Une correspondance exacte est requise.

7. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

Le tableau suivant décrit les champs en lecture seule de la page.

Table 160 : Informations statistiques du service DiffServ

Champ	Description
Interface	Interface avec une stratégie DiffServ attachée.
Direction	Direction (entrée ou sortie) à laquelle la politique DiffServ est associée.
Nom de la politique	Nom de la stratégie DiffServ. Si plusieurs classes sont associées à la stratégie, chaque instance de stratégie (portant le même nom de stratégie) s'affiche.
Statut opérationnel	État opérationnel de la stratégie DiffServ (haut ou bas). L'état est affiché comme UP si toutes les conditions suivantes sont remplies : • La classe attachée est valide et inclut au moins une règle correspondante. • La stratégie associée est valide et inclut au moins un attribut. • Le port est activé, c'est-à-dire que la liaison physique du port est à l'état <i>actif</i>.
Classes membres	Toutes les classes DiffServ définies comme membres du nom de stratégie sélectionné. Sélectionnez un nom de classe membre pour afficher ses statistiques. Si aucune classe n'est associée à la règle sélectionnée, la liste est vide.
Paquets offerts	Nombre total de paquets offerts à toutes les instances de classe sur cette stratégie de service avant que leur traitement de stratégie DiffServ défini ne soit appliqué. Il s'agit du nombre total pour l'interface et la direction.
Paquets supprimés	Nombre total de paquets rejetés pour quelque raison que ce soit pour toutes les instances de classe de cette stratégie de service lorsque le traitement de stratégie DiffServ est appliqué. Il s'agit du nombre total pour l'interface et la direction.

9

Gérer la sécurité du commutateur

Il aborde les sujets suivants :

- Comptes utilisateur et mots de passe
- serveurs RADIUS
- Serveurs TACACS+
- Listes d'authentification
- Sessions de connexion en cours
- Accès de gestion HHTP et HTTPS
- Accès de gestion SSH
- Accès à la gestion Telnet
- Accès à la gestion des ports de console
- Déni de service
- Profils et règles d'accès de gestion
- Authentification du port
- Filtres MAC pour le contrôle du trafic
- Sécurité portuaire
- Groupe de ports privés
- Protection des ports
- VLAN privés
- Storm Control
- Protocole DHCP Snooping
- Surveillance DHCPv6
- Interfaces IP source Guard

- Interfaces de protection source IPv6
- Inspection ARP dynamique
- Portail captif
- Liste de contrôle d'accès

Comptes utilisateur et mots de passe

Vous pouvez configurer des comptes utilisateur et des mots de passe de connexion. Par défaut, deux comptes utilisateur existent :

- admin, avec privilèges de lecture et d'écriture (lecture/écriture)
- invité, avec privilèges de lecture seule

Les noms de compte ne sont pas sensibles à la casse.

La première fois que vous vous connectez en tant qu'administrateur à l'interface utilisateur principale, aucun mot de passe n'est requis (c'est-à-dire que le mot de passe est vide). Après vous être connecté pour la première fois, vous devez spécifier un mot de passe de périphérique local que vous devez ensuite utiliser pour vous reconnecter. Chaque fois que vous vous connectez ultérieurement, vous devez utiliser le mot de passe de votre périphérique local.

Un utilisateur invité ne peut pas se connecter tant que l'utilisateur admin n'a pas spécifié un mot de passe pour l'utilisateur invité.

Si vous vous connectez en tant qu'utilisateur administrateur avec des privilèges de lecture/écriture, vous pouvez attribuer des mots de passe, définir des paramètres de sécurité pour les comptes par défaut et ajouter et supprimer des comptes (autres que le compte administrateur), jusqu'à un maximum de six comptes. En tant qu'utilisateur administrateur disposant de privilèges de lecture/écriture, vous modifiez toutes les données des pages principales de l'interface utilisateur.

Ajouter ou modifier un compte utilisateur

Vous pouvez ajouter ou modifier un compte utilisateur, y compris les comptes utilisateur prédéfinis *admin* et *guest*.

Pour ajouter ou modifier un compte utilisateur :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.
4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **sécurité > gestion sécurité > utilisateur local > gestion des utilisateurs** .
La page gestion des utilisateurs s'affiche.
6. Si vous modifiez les paramètres d'un compte d'utilisateur existant, cochez la case correspondant au compte d'utilisateur.
Vous ne pouvez pas modifier le nom d'un compte utilisateur existant.
7. Si vous ajoutez un nouveau compte utilisateur, saisissez un nom dans le champ **nom d'utilisateur**.
Vous ne pouvez entrer un nom d'utilisateur que lorsque vous créez un compte. Les noms d'utilisateur peuvent contenir jusqu'à 64 caractères et ne sont pas sensibles à la casse. Les caractères valides incluent tous les caractères alphanumériques ainsi que les tirets (-) et les traits de soulignement (_). Le nom d'utilisateur par défaut n'est pas valide. Une fois créés, les noms d'utilisateur ne peuvent pas être modifiés ou modifiés.
8. Dans le menu **modifier le mot de passe**, sélectionnez **Activer**.
Par défaut, la sélection est désactiver. Activez cette option uniquement si vous définissez ou modifiez les options de mot de passe.
9. Dans le champ **Password** (Mot de passe), entrez le mot de passe de la connexion FAI.
Les caractères ne s'affichent pas au fur et à mesure qu'ils sont saisis ; seuls les astérisques (*) s'affichent. Les mots de passe comportent jusqu'à huit caractères alphanumériques et sont sensibles à la casse.
10. Dans le champ **confirmer le mot de** passe, saisissez à nouveau le mot de passe pour confirmer que vous avez saisi informatique correctement.

Ce champ n'affiche pas le mot de passe lorsque informatique est tapé, mais affiche des astérisques (*).

11. Dans le menu **mode d'accès**, sélectionnez **lecture_écriture** ou **lecture_seule**.
12. Dans le menu **type de cryptage**, sélectionnez le niveau de cryptage :
 - SHA256 : Algorithme de hachage sécurisé compatible avec de nombreux périphériques.
 - SHA512 : Algorithme de hachage sécurisé supérieur à SHA256. Il s'agit du type par défaut.
13. Dans le menu **mode d'authentification multifacteur**, sélectionnez pour activer ou désactiver l'authentification multifacteur :
 - Désactiver : L'authentification multifacteur est désactivée. Il s'agit de la sélection par défaut.
 - Activer. L'authentification multifacteur est activée et un e-mail d'authentification est envoyé à l'adresse e-mail que vous devez saisir dans le champ **informations sur l'e-mail d'authentification multifacteur**.
14. Effectuez l'une des opérations suivantes :
 - Si vous ajoutez un nouveau compte utilisateur, cliquez sur le bouton **Ajouter**. Les paramètres sont enregistrés. Le compte utilisateur est ajouté.
 - Si vous modifiez les paramètres d'un compte utilisateur, cliquez sur le bouton **appliquer**. Les paramètres sont enregistrés.
15. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 161 : Informations de gestion des utilisateurs

Champ	Description
État de verrouillage	Indique si le compte utilisateur est verrouillé (vrai ou faux)
Date d'expiration du mot de passe	Date d'expiration du mot de passe, le cas échéant

Supprimer un compte utilisateur

Vous pouvez supprimer un compte utilisateur qui n'est plus nécessaire.

Pour supprimer un compte utilisateur :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > gestion sécurité > utilisateur local > gestion des utilisateurs**.

La page gestion des utilisateurs s'affiche.

6. Cochez les cases correspondant au contenu.

7. Cliquez sur le bouton **Supprimer**.

L'utilisateur est supprimé.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurer les exigences de mot de passe utilisateur

Pour configurer les exigences de mot de passe utilisateur :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > gestion de la sécurité > utilisateur local > Configuration du mot de passe utilisateur**.

La page Configuration du mot de passe utilisateur s'affiche.

6. Dans le champ **longueur minimale du mot de passe**, saisissez la longueur minimale de caractères pour tout nouveau mot de passe utilisateur local.

La valeur par défaut est de huit caractères. La plage est de 0 à 64 secondes.

7. Dans le champ **expiration du mot de passe (jours)**, saisissez le nombre maximal de jours pendant lesquels un mot de passe utilisateur est valide, à compter du jour où le mot de passe est défini.

Après expiration d'un mot de passe, l'utilisateur doit définir un nouveau mot de passe lors de la connexion. La valeur par défaut est 0, ce qui signifie que les mots de passe n'expirent pas. La plage est de 0 à 365 secondes.

8. Dans le champ **historique des mots de passe**, saisissez le nombre de mots de passe précédents que le commutateur stocke pour empêcher les utilisateurs de les réutiliser. La valeur par défaut est 0, ce qui signifie que le commutateur ne stocke pas les mots de passe précédents. La plage est de 0 à 10 secondes.

9. Dans le champ **tentatives de verrouillage**, spécifiez le nombre de fois qu'un utilisateur est autorisé à échouer une tentative d'authentification locale avant que le compte d'utilisateur ne soit verrouillé. La valeur par défaut est 5 fois. Si vous entrez 0, une tentative d'authentification locale échouée n'entraîne pas le verrouillage du compte utilisateur. La plage est de 0 à 5 secondes.

10. Dans le champ **heure de déverrouillage**, spécifiez la durée en minutes après laquelle un compte utilisateur verrouillé est déverrouillé. La valeur par défaut est 5 minutes. La plage est de 1 à 60 secondes.

11. Sélectionnez un bouton radio déverrouiller le mode minuterie pour activer ou désactiver le verrouillage d'un compte utilisateur après un trop grand nombre de tentatives de connexion infructueuses :

- Désactiver : Un compte utilisateur n'est jamais verrouillé.
- Activer. Un compte utilisateur est verrouillé pendant un certain temps après un trop grand nombre de tentatives de connexion infructueuses.

Après avoir saisi un mot de passe erroné trois fois, le commutateur bloque les tentatives de connexion ultérieures. Le blocage dure plus longtemps à chaque fois jusqu'à ce que vous obteniez le mot de passe correct :

- Après 3 fois : 5 minutes
- Au bout de 6 fois : 10 minutes
- Après 9 fois : 20 minutes
- Après 12 fois : 40 minutes
- Après 15 fois : 60 minutes
- Après 18 fois : 60 minutes

12. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

13. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Activez l'authentification multifacteur sur le commutateur

Si vous activez l'authentification multifacteur (MFA) sur le commutateur, informatique s'applique aux types d'accès suivants :

- Interface utilisateur principale :
- Accès CLI via Telnet
- Accès CLI via SSH

MFA ne s'applique pas à l'accès à la console.

Vous pouvez configurer MFA pour un utilisateur individuel (voir [Ajouter ou modifier un compte utilisateur](#) à la page 820) et configurer l'adresse e-mail utilisée pour les mots de passe à usage unique (OTP), mais pour que MFA prenne effet, MFA doit également être activé globalement sur le commutateur.

Pour plus d'informations sur l'utilisation de l'interface de ligne de commande pour configurer un serveur de messagerie sur le commutateur, reportez-vous au manuel de l'interface de ligne de commande que vous téléchargez sur le site netgear.com/support/download/.

Pour activer l'authentification multifacteur sur le commutateur :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **sécurité > gestion de la sécurité > utilisateur local > Configuration globale MFA** .
La page Configuration globale MFA s'affiche.
6. Sélectionnez un bouton radio mode d'authentification multifacteur pour activer ou désactiver l'authentification multifacteur :
 - Désactiver : L'authentification multifacteur est désactivée sur le commutateur. Il s'agit de l'option par défaut.
 - Activer. L'authentification multifacteur est activée sur le commutateur.
7. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Modifiez le mot de passe CLI d'exécution privilégiée

Vous pouvez modifier le mot de passe d'exécution privilégié pour accéder au mode d'exécution privilégié dans l'interface de ligne de commande (CLI). Les mots de passe doivent comporter au maximum 64 caractères alphanumériques. Le mot de passe est sensible à la casse. Vous pouvez également modifier le niveau de cryptage.

Pour modifier le mot de passe CLI d'exécution privilégiée à utiliser dans l'interface CLI et le niveau de cryptage :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > sécurité de gestion > Activer le mot de passe**.

La page Activer le mot de passe s'affiche.

6. Dans le menu **type de cryptage**, sélectionnez le niveau de cryptage :

- SHA256 : Algorithme de hachage sécurisé compatible avec de nombreux périphériques.
- SHA512 : Algorithme de hachage sécurisé supérieur à SHA256. Il s'agit du type par défaut.

7. Dans le champ **mot de passe**, saisissez le mot de passe.

Le mot de passe peut contenir jusqu'à 64 caractères alphanumériques.

8. Dans le champ **confirmer le mot de** passe, saisissez à nouveau le mot de passe pour confirmer que vous avez entré informatique correctement.

9. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Modifiez le mot de passe de la console, Telnet ou SSH

Un mot de passe de ligne est un mot de passe utilisé pour l'accès à la console, Telnet ou SSH.

Vous pouvez modifier un mot de passe et le niveau de cryptage.

Pour configurer le mot de passe de la console, Telnet ou SSH et le niveau de cryptage :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > sécurité de gestion > mot de passe de ligne** .

La page mot de passe de ligne s'affiche.

6. Pour modifier le mot de passe de la console et le niveau de cryptage, procédez comme suit :

- a. Cochez la case **Console**.

- b. Dans le menu **type de cryptage**, sélectionnez le niveau de cryptage :

- SHA256 : Algorithme de hachage sécurisé compatible avec de nombreux périphériques.
- SHA512 : Algorithme de hachage sécurisé supérieur à SHA256. Il s'agit du type par défaut.

- c. Dans le champ **mot de passe de la console**, saisissez le mot de passe de la console.

Le mot de passe peut contenir jusqu'à 64 caractères alphanumériques.

- d. Dans le champ **confirmer le mot de passe de la console**, saisissez à nouveau le mot de passe pour confirmer que vous avez saisi informatique correctement.
7. Pour modifier le mot de passe Telnet et le niveau de cryptage, procédez comme suit :
 - a. Cochez la case **Telnet**.
 - b. Dans le menu **type de cryptage**, sélectionnez le niveau de cryptage :
 - SHA256 : Algorithme de hachage sécurisé compatible avec de nombreux périphériques.
 - SHA512 : Algorithme de hachage sécurisé supérieur à SHA256. Il s'agit du type par défaut.
 - c. Dans le champ **mot de passe de la console**, saisissez le mot de passe de la console.

Le mot de passe peut contenir jusqu'à 64 caractères alphanumériques.
 - d. Dans le champ **confirmer le mot de passe de la console**, saisissez à nouveau le mot de passe pour confirmer que vous avez saisi informatique correctement.
8. Pour modifier le mot de passe SSH et le niveau de cryptage, procédez comme suit :
 - a. **Activez la case à cocher** SSH.
 - b. Dans le menu **type de cryptage**, sélectionnez le niveau de cryptage :
 - SHA256 : Algorithme de hachage sécurisé compatible avec de nombreux périphériques.
 - SHA512 : Algorithme de hachage sécurisé supérieur à SHA256. Il s'agit du type par défaut.
 - c. Dans le champ **mot de passe de la console**, saisissez le mot de passe de la console.

Le mot de passe peut contenir jusqu'à 64 caractères alphanumériques.
 - d. Dans le champ **confirmer le mot de passe de la console**, saisissez à nouveau le mot de passe pour confirmer que vous avez saisi informatique correctement.
9. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.
10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

serveurs RADIUS

Les serveurs RADIUS offrent une sécurité supplémentaire aux réseaux. Le serveur RADIUS gère une base de données utilisateur, qui contient des informations d'authentification par utilisateur. Le commutateur transmet les informations au serveur RADIUS configuré, qui peut authentifier un nom d'utilisateur et un mot de passe avant d'autoriser l'utilisation du réseau. Les serveurs RADIUS fournissent une méthode d'authentification centralisée pour les éléments suivants :

- Accès Web
- Contrôle d'accès aux ports (802.1X)

Configurez les paramètres globaux du serveur RADIUS.

Vous pouvez ajouter des informations sur plusieurs serveurs RADIUS sur le réseau.

Si vous configurez plusieurs serveurs RADIUS, tenez compte du délai maximal lorsque vous spécifiez le nombre maximal de retransmissions (c'est-à-dire la valeur que vous entrez dans le champ **nombre maximal de retransmissions** dans la procédure suivante) et la période de temporisation (c'est-à-dire la valeur que vous entrez dans le champ **durée de temporisation** dans la procédure suivante) pour RADIUS :

- Pour un serveur RADIUS, une retransmission n'a lieu qu'après expiration du délai configuré sans réponse du serveur RADIUS. En outre, le nombre maximal de retransmissions pour un serveur RADIUS doit être passé avant que le commutateur tente de passer au serveur RADIUS suivant.
- Par conséquent, le délai maximal de réception d'une réponse RADIUS sur le commutateur est égal au nombre maximal de retransmissions multiplié par la période d'expiration multipliée par le nombre de serveurs RADIUS configurés. Si la requête RADIUS a été générée par une tentative de connexion utilisateur, toutes les interfaces utilisateur sont bloquées jusqu'à ce que le commutateur reçoive une réponse RADIUS.

Configurez les paramètres globaux du serveur RADIUS.

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > sécurité de gestion > RADIUS > Configuration globale**.

La page Configuration globale s'affiche.

Le champ Current Server Address (adresse du serveur actuel) est vide si aucun serveur n'est configuré (voir [Configurez un serveur d'authentification RADIUS sur le commutateur](#), à la page 834).

Le commutateur prend en charge jusqu'à trois serveurs RADIUS configurés. Si plusieurs serveurs RADIUS sont configurés, le serveur actuel est le serveur principal. Si aucun serveur n'est configuré comme serveur principal, le serveur actuel est le serveur RADIUS le plus récemment ajouté.

6. Dans le menu **interface source**, sélectionnez l'interface source que le commutateur doit utiliser pour communiquer avec les serveurs RADIUS. Par défaut, les options suivantes s'affichent dans le menu :

- Aucun : L'adresse IP principale de l'interface d'origine (sortante) est utilisée comme adresse source.
- VLAN 1 L'adresse IP principale de VLAN 1 est utilisée comme adresse source. Il s'agit de la sélection par défaut.
- Port de service L'adresse IP du port de gestion est utilisée comme adresse source.

Selon la configuration de votre commutateur, les options suivantes peuvent s'afficher :

- **Un autre identifiant VLAN** : L'adresse IP principale d'un VLAN autre que VLAN 1 est utilisée comme adresse source.
 - **Interface de routage** : L'adresse IP principale d'une interface de routage est utilisée comme adresse source.
 - **VLAN de routage** : L'adresse IP principale d'une interface de routage VLAN est utilisée comme adresse source.
 - **Interface de bouclage de routage** : L'adresse IP principale d'une interface de bouclage de routage est utilisée comme adresse source.
 - **Différent** : Pour certaines fonctionnalités, *différents* peuvent s'afficher. Cela signifie que l'interface source est configurée séparément.
7. Dans le champ **nombre maximal de retransmissions**, spécifiez le nombre maximal de **retransmissions** d'un paquet de requête au serveur RADIUS.
La plage est de 1 à 15. La valeur par défaut est 4.
-  **Attention:** Le délai maximal de réception d'une réponse RADIUS sur le commutateur est égal au nombre maximal de retransmissions multiplié par la période d'expiration multipliée par le nombre de serveurs RADIUS configurés. Si la requête RADIUS a été générée par une tentative de connexion utilisateur, toutes les interfaces utilisateur sont bloquées jusqu'à ce que le commutateur reçoive une réponse RADIUS.
8. Dans le champ **durée du délai d'attente**, spécifiez la valeur du délai d'attente, en secondes, pour les retransmissions de demandes.
La plage est de 1 à 30. La valeur par défaut est 5.
9. Sélectionnez le bouton radio désactiver ou Activer le mode EEE.
Cette sélection spécifie si le mode de comptabilité RADIUS est activé sur le serveur actuel. Par défaut, la sélection est désactiver.
10. Sélectionnez le bouton radio **désactiver** ou **Activer** le mode attribut RADIUS 4.
Cette sélection spécifie si l'attribut RADIUS 4 est activé sur le serveur actuel. Par défaut, la sélection est désactiver. Si vous sélectionnez le bouton radio **Activer**, le champ **valeur attribut RADIUS 4** s'affiche, vous permettant de saisir une adresse IPv4 pour l'option attribut RADIUS 4.
11. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
12. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 162 : Informations de configuration RADIUS

Champ	Description
Adresse actuelle du serveur	Adresse du serveur RADIUS actuel. Ce champ est vide si aucun serveur n'est configuré.
Nombre de serveurs d'authentification configurés	Nombre de serveurs RADIUS d'authentification configurés. Cette valeur doit être comprise entre 0 et 32.
Nombre de serveurs de comptabilité configurés	Nombre de serveurs de comptabilité RADIUS configurés. Cette valeur doit être comprise entre 0 et 32.
Nombre de groupes de serveurs d'authentification nommés	Nombre de groupes d'authentification de serveur RADIUS nommés configurés.
Nombre de groupes de serveurs de comptabilité nommés	Nombre de groupes comptables de serveur RADIUS nommés configurés.

Configurez un serveur d'authentification RADIUS sur le commutateur.

Vous pouvez configurer et afficher divers paramètres de communication entre le commutateur et un serveur d'authentification RADIUS.

Ajoutez un serveur d'authentification RADIUS au commutateur

Vous pouvez ajouter des informations sur un serveur d'authentification RADIUS au commutateur et afficher ou réinitialiser les statistiques du serveur d'authentification RADIUS.

Pour ajouter un serveur d'authentification RADIUS au commutateur et afficher ou réinitialiser les statistiques du serveur d'authentification RADIUS :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **sécurité > sécurité de gestion > RADIUS > Configuration du serveur**.
La page Configuration du serveur SNTP s'affiche.
6. Dans le champ **adresse IP du serveur RADIUS**, spécifiez l'adresse IP du serveur RADIUS.
7. Dans le champ **nom du serveur RADIUS**, spécifiez un nom pour le serveur RADIUS.
Ce nom vous aide à identifier le serveur RADIUS.
8. Dans le champ **Port**, spécifiez le numéro de port UDP du serveur d'authentification RADIUS.
La plage est de 1 à 65535.
9. Dans le menu **secret configuré**, sélectionnez **Oui**.
Vous devez sélectionner **Oui** avant de pouvoir configurer le secret RADIUS. Une fois le serveur RADIUS ajouté, ce champ indique si le secret partagé pour ce serveur a été configuré.
10. Dans le champ **secret**, saisissez la chaîne de texte secrète partagée utilisée pour authentifier et chiffrer toutes les communications RADIUS entre le commutateur et le serveur RADIUS.
Ce secret doit correspondre à celui configuré sur le serveur RADIUS.
11. Dans le menu **match Every**, sélectionnez l'une des options suivantes :
 - **Oui**: Le serveur fonctionne comme le serveur d'authentification RADIUS principal.
 - **Non**: Le serveur fonctionne comme un serveur d'authentification RADIUS secondaire.

12. Dans le menu **authentificateur de message**, sélectionnez **Activer** ou **désactiver** pour spécifier si l'attribut authentificateur de message pour le serveur sélectionné est activé.

L'authentificateur de message ajoute une protection aux messages RADIUS en utilisant un hachage MD5 pour crypter chaque message. Le secret partagé est utilisé comme clé, et si le message ne peut pas être vérifié par le serveur RADIUS, informatique est ignoré.

13. Dans le menu **match Every**, sélectionnez l'une des options suivantes :

- Netgear Un serveur RADIUS spécifique à NETGEAR.
- Standard Un serveur RADIUS tiers.

14. Cliquez sur le bouton **Add** (Ajouter).

Le serveur est ajouté au commutateur.

15. Pour rétablir les valeurs par défaut du serveur d'authentification et des statistiques RADIUS, cliquez sur le bouton **Effacer les compteurs**.

16. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le champ actuel indique si le serveur est actuellement utilisé comme serveur d'authentification RADIUS.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 163 : Informations statistiques du serveur d'authentification RADIUS

Champ	Description
Serveur RADIUS	Adresse du serveur RADIUS ou nom du serveur RADIUS pour lequel les statistiques sont affichées
Temps aller-retour	Intervalle de temps, en centièmes de seconde, entre la réponse d'accès/défi d'accès la plus récente et la demande d'accès correspondant à informatique de ce serveur d'authentification RADIUS
Demandes d'accès	Nombre de paquets de demande d'accès RADIUS envoyés à ce serveur. Ce numéro n'inclut pas les retransmissions.
Accéder aux retransmissions	Nombre de paquets de demande d'accès RADIUS retransmis à ce serveur
Access accepte	Nombre de paquets RADIUS Access-Accept, y compris les paquets valides et non valides, reçus de ce serveur
Refus d'accès	Nombre de paquets RADIUS de rejet d'accès, y compris les paquets valides et non valides, reçus de ce serveur
Défis d'accès	Nombre de paquets de demande d'accès RADIUS, y compris les paquets valides et non valides, reçus de ce serveur

Table 163 : Informations statistiques du serveur d'authentification RADIUS (A continué)

Champ	Description
Réponses d'accès mal formées	Nombre de paquets RADIUS de réponse d'accès mal formés reçus de ce serveur. Les paquets mal formés comprennent des paquets dont la longueur n'est pas valide. Les authenticateurs ou attributs de signature incorrects ou les types inconnus ne sont pas inclus dans les réponses d'accès mal formées.
Authenticateurs incorrects	Nombre de paquets RADIUS Access-Response contenant des authenticateurs ou des attributs de signature non valides reçus de ce serveur
Demandes en attente	Nombre de paquets de demande d'accès RADIUS destinés à ce serveur qui n'ont pas encore expiré ou qui n'ont pas reçu de réponse
Dépassement du délai imparti	Nombre de délais d'expiration de l'authentification pour ce serveur
Types inconnus	Nombre de paquets RADIUS de type inconnu reçus de ce serveur sur le port d'authentification
Paquets abandonnés	Nombre de paquets RADIUS reçus de ce serveur sur le port d'authentification et abandonnés pour une autre raison

Modifiez les paramètres d'un serveur d'authentification RADIUS sur le commutateur

Vous pouvez modifier les paramètres d'un serveur d'authentification RADIUS sur le commutateur.

Pour modifier les paramètres d'un serveur d'authentification RADIUS sur le commutateur :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > sécurité de gestion > RADIUS > Configuration du serveur**

.

La page Configuration du serveur SNTP s'affiche.

6. Cochez la case en regard du numéro du IP.
7. Modifiez la configuration du serveur sélectionné.
8. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimez un serveur d'authentification RADIUS du commutateur

Si vous n'avez plus besoin d'un serveur d'authentification RADIUS, vous pouvez supprimer informatiquement le serveur du commutateur.

Pour supprimer un serveur d'authentification RADIUS du commutateur :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **sécurité > sécurité de gestion > RADIUS > Configuration du serveur**.
La page Configuration du serveur SNTP s'affiche.
6. Cochez la case en regard de l'adresse IP du serveur.
7. Cliquez sur le bouton **Supprimer**.
Le serveur RADIUS est supprimé.
8. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez un serveur d'authentification RADIUS sur le commutateur.

Vous pouvez configurer et afficher divers paramètres de communication entre le commutateur et un serveur de comptabilité RADIUS.

Ajoutez un serveur de comptabilité RADIUS au commutateur

Vous pouvez ajouter des informations sur un serveur de comptabilité RADIUS au commutateur et afficher ou réinitialiser les statistiques du serveur de comptabilité RADIUS.

Pour ajouter un serveur de comptabilité RADIUS au commutateur et afficher ou effacer les statistiques du serveur de comptabilité RADIUS :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > sécurité de gestion > RADIUS > Configuration du serveur de comptabilité**.

La page Accounting Server Configuration s'affiche.

6. Dans le champ **adresse IP du serveur de comptabilité**, spécifiez l'adresse IP du serveur de comptabilité RADIUS.
7. Dans le champ **nom du serveur de comptabilité**, entrez le nom du serveur de comptabilité.
8. Dans le champ **Port**, spécifiez le numéro de port UDP du serveur de comptabilité RADIUS.
La plage est de 1 à 65535.
9. Dans le menu **secret configuré**, sélectionnez **Oui** pour ajouter un secret RADIUS dans le champ suivant.

Après avoir ajouté le serveur de comptabilité RADIUS, ce champ indique si le secret partagé pour ce serveur est configuré.

10. Dans le champ **secret**, saisissez le secret partagé à utiliser avec le serveur de comptabilité spécifié.
11. Dans le menu **mode comptabilité**, sélectionnez pour activer ou désactiver le mode comptabilité RADIUS :
 - Activer. Tous les serveurs de comptabilité RADIUS configurés sont activés sur le commutateur.
 - Désactiver : Tous les serveurs de comptabilité RADIUS configurés sont désactivés sur le commutateur.

! Remarque: Votre sélection dans le menu **mode comptabilité** s'applique à tous les serveurs de comptabilité configurés, pas seulement au serveur que vous ajoutez.

12. Cliquez sur le bouton **Add** (Ajouter).

Le serveur est ajouté au commutateur.

13. Pour rétablir les valeurs par défaut du serveur d'authentification et des statistiques RADIUS, cliquez sur le bouton **Effacer les compteurs**.

14. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 164 : Informations statistiques du serveur de comptabilité RADIUS

Champ	Description
Serveur de comptabilité	Serveur de comptabilité associé aux statistiques
Temps aller-retour	Intervalle de temps, en centièmes de seconde, entre la réponse comptable la plus récente et la demande comptable correspondant à informatique de ce serveur de comptabilité RADIUS
Demandes comptables	Nombre de paquets RADIUS de demandes de comptabilité envoyés, retransmissions non comprises
Retransmissions comptables	Nombre de paquets de demandes de comptabilité RADIUS retransmis à ce serveur de comptabilité RADIUS
Réponses comptables	Nombre de paquets RADIUS reçus sur le port de comptabilité de ce serveur
Réponses comptables mal formées	Nombre de paquets RADIUS de réponse comptable mal formés reçus de ce serveur. Les paquets mal formés comprennent des paquets dont la longueur n'est pas valide. Les authenticateurs incorrects et les types inconnus ne sont pas inclus comme réponses comptables mal formées.
Authenticateurs incorrects	Nombre de paquets RADIUS Accounting-Response contenant des authenticateurs non valides reçus de ce serveur de comptabilité

Table 164 : Informations statistiques du serveur de comptabilité RADIUS (A continué)

Champ	Description
Demandes en attente	Nombre de paquets RADIUS de demandes de comptabilité envoyés à ce serveur qui n'ont pas encore expiré ou qui n'ont pas reçu de réponse
Dépassement du délai imparti	Le nombre de délais de comptabilisation pour ce serveur
Types inconnus	Nombre de paquets RADIUS de type inconnu reçus de ce serveur sur le port de comptabilité
Paquets abandonnés	Nombre de paquets RADIUS reçus de ce serveur sur le port de comptabilité et abandonnés pour une autre raison

Modifiez les paramètres d'un serveur de comptabilité RADIUS sur le commutateur

Vous pouvez modifier les paramètres d'un serveur de comptabilité RADIUS sur le commutateur.

Pour modifier les paramètres d'un serveur de comptabilité RADIUS sur le commutateur :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **sécurité > sécurité de gestion > RADIUS > Configuration du serveur de comptabilité** .
La page Accounting Server Configuration s'affiche.
6. Cochez la case en regard du numéro du IP.
7. Modifiez la configuration du serveur de comptabilité.
8. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimez un serveur de comptabilité RADIUS du commutateur

Si vous n'avez plus besoin d'un serveur de comptabilité RADIUS, vous pouvez supprimer informatique du commutateur.

Pour supprimer un serveur de comptabilité RADIUS du commutateur :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **sécurité > sécurité de gestion > RADIUS > Configuration du serveur de comptabilité**.
La page Accounting Server Configuration s'affiche.
6. Cochez la case en regard du numéro du IP.
7. Cliquez sur le bouton **Supprimer**.
Les paramètres sont enregistrés. Le serveur de comptabilité RADIUS est supprimé.
8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Serveurs TACACS+

TACACS+ fournit un système de gestion des utilisateurs centralisé, tout en conservant la cohérence avec RADIUS et les autres processus d'authentification. TACACS+ fournit les services suivants :

- **Authentification.** Fournit une authentification lors de la connexion et via des noms d'utilisateur et des mots de passe définis par l'utilisateur.
- Autorisation Effectué à la connexion. Lorsque la session d'authentification est terminée, une session d'autorisation commence avec le nom d'utilisateur authentifié. Le serveur TACACS+ vérifie les privilèges de l'utilisateur.

Le protocole TACACS+ assure la sécurité du réseau grâce à des échanges de protocole cryptés entre l'appareil et le serveur TACACS+.

Configurez les paramètres TACACS+ globaux

Vous pouvez configurer les paramètres TACACS+ globaux pour la communication entre le commutateur et un serveur TACACS+.

Pour configurer les paramètres TACACS+ globaux :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > sécurité de gestion > TACACS > Configuration TACACS+**

L'écran TACACS Configuration (Configuration IP) s'affiche.

6. Dans le champ **Key String**, spécifiez la clé d'authentification et de cryptage pour les communications TACACS+ entre le commutateur et le serveur TACACS+.

La plage est de 0 à 128. La clé doit correspondre à la clé configurée sur le serveur TACACS+.

7. Dans le champ **délai de connexion**, spécifiez le nombre maximal de secondes autorisé pour établir une connexion TCP entre le commutateur et le serveur TACACS+.

La plage est de 1 à 30 secondes. La valeur par défaut est de 5 secondes.

8. Dans le menu **interface source**, sélectionnez l'interface source à utiliser pour la communication TACACS+. Par défaut, les options suivantes s'affichent dans le menu :

- **Aucun** : L'adresse IP principale de l'interface d'origine (sortante) est utilisée comme adresse source.
- **VLAN 1** : L'adresse IP principale de VLAN 1 est utilisée comme adresse source. Il s'agit de la sélection par défaut.
- **Port de service** : L'adresse IP du port de gestion est utilisée comme adresse source.

Selon la configuration de votre commutateur, les options suivantes peuvent s'afficher :

- **Un autre identifiant VLAN** : L'adresse IP principale d'un VLAN autre que VLAN 1 est utilisée comme adresse source.
- **Interface de routage** : L'adresse IP principale d'une interface de routage est utilisée comme adresse source.
- **VLAN de routage** : L'adresse IP principale d'une interface de routage VLAN est utilisée comme adresse source.
- **Interface de bouclage de routage** : L'adresse IP principale d'une interface de bouclage de routage est utilisée comme adresse source.
- **Différent** : Pour certaines fonctionnalités, *différents* peuvent s'afficher. Cela signifie que l'interface source est configurée séparément.

9. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Ajoutez un serveur TACACS+ au commutateur

Vous pouvez ajouter jusqu'à cinq serveurs TACACS+ avec lesquels le commutateur peut communiquer.

Pour ajouter un serveur TACACS+ au commutateur :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.
4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **sécurité > sécurité de gestion > TACACS > Configuration du serveur TACACS+** .
La page TACACS+ Server Configuration s'affiche.
6. Dans le champ **serveur TACACS+**, entrez l'adresse IP du serveur TACACS+.
7. Dans le champ **priorité**, spécifiez la priorité du serveur TACACS+.
La priorité détermine l'ordre dans lequel les serveurs TACACS+ sont contactés lors de la tentative d'authentification d'un utilisateur. La valeur 0 est la priorité la plus élevée. La plage est de 0 à 65535.
8. Dans le champ **Port**, spécifiez le numéro de port d'authentification pour les sessions serveur TACACS+.
Le numéro de port doit être compris entre 0 et 65535.
9. Dans le champ **chaîne de clé**, spécifiez la clé d'authentification et de cryptage pour les communications TACACS+ entre le terminal et le serveur TACACS+.
L'étiquette de nom peut comporter de 0 à 128 caractères. La clé doit correspondre à la clé utilisée sur le serveur TACACS+.
10. Dans le champ **délai de connexion**, spécifiez le délai qui s'écoule avant l'expiration de la connexion entre le périphérique et le serveur TACACS+.
La plage est de 1 à 30 secondes.
11. Cliquez sur le bouton **Add** (Ajouter).
Le serveur est ajouté au commutateur.
12. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Modifiez les paramètres d'un serveur TACACS+ sur le commutateur .

Modifiez les paramètres d'un serveur TACACS+ sur le commutateur .

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > sécurité de gestion > TACACS+ > Configuration du serveur TACACS+** .

La page TACACS+ Server Configuration s'affiche.

6. Cochez la case en regard du numéro du IP.
7. Modifiez la configuration du serveur TACACS+ sélectionné.
8. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimez un serveur TACACS+ du commutateur.

Supprimez un serveur TACACS+ du commutateur.

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > sécurité de gestion > TACACS+ > Configuration du serveur TACACS+** .

La page TACACS+ Server Configuration s'affiche.

6. Cochez la case en regard du numéro du IP.

7. Cliquez sur le bouton **Supprimer**.

Le serveur TACACS+ est supprimé.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Listes d'authentification

Une liste de connexion d'authentification spécifie une ou plusieurs méthodes d'authentification pour valider l'accès au commutateur ou au port pour un utilisateur administrateur ou invité. L'accès peut être un accès HTTP ou HTTPS à l'interface utilisateur principale ou à l'interface utilisateur AV, ou un accès de ligne (c'est-à-dire Telnet, SSH ou accès console) à l'interface de ligne de commande.

Configurez une liste d'authentification de connexion

Une liste de connexion spécifie les méthodes d'authentification à utiliser pour valider l'accès au commutateur ou au port. Une liste d'authentification peut s'appliquer aux utilisateurs qui accèdent au commutateur par l'une des méthodes suivantes :

- SSH (Secure Shell) Pour plus d'informations sur la sélection d'une liste d'authentification pour l'accès SSH, reportez-vous à la section [Accès de gestion SSH](#) à la page 875.
- Telnet Pour plus d'informations sur la sélection d'une liste d'authentification pour l'accès Telnet, reportez-vous à la section [Accès à la gestion Telnet](#) à la page 883.
- Port console Pour plus d'informations sur la sélection d'une liste d'authentification pour l'accès au port de console, reportez-vous à [Accès à la gestion des ports de console](#) à la page 887 la section .

Deux listes par défaut sont présentes : defaultList et NetworkList. Vous ne pouvez pas supprimer ces listes. Par défaut, les utilisateurs préconfigurés (admin et guest) sont affectés à ces deux listes de la manière suivante :

- Pour l'accès SSH et Telnet, par défaut, les utilisateurs préconfigurés sont affectés à la liste par défaut.
- Pour l'accès à la console, par défaut, les utilisateurs préconfigurés sont affectés à la NetworkList.

Tous les utilisateurs nouvellement ajoutés sont également affectés à la liste par défaut jusqu'à ce que vous les assigniez spécifiquement à une autre liste (voir [Configurez les paramètres d'authentification 802.1X globaux](#) à la page 900).

Pour configurer une liste d'authentification de connexion :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > sécurité de gestion > liste d'authentification > liste d'authentification de connexion**.

La page Login Authentication List s'affiche.

6. Effectuez l'une des opérations suivantes :

- **Créer une nouvelle liste** : Dans le champ **nom de la liste**, spécifiez un nom. Le nom peut comporter jusqu'à 15 caractères et est sensible à la casse.
- **Modifier une liste existante** : Cochez la case associée à la liste.

7. Dans le menu de la colonne **1**, sélectionnez la méthode d'authentification à utiliser en premier dans la liste de connexion d'authentification sélectionnée.

Si vous sélectionnez une méthode qui n'expire pas comme première méthode, telle que locale, aucune autre méthode n'est essayée, même si vous avez spécifié plusieurs méthodes. L'authentification de l'utilisateur se produit dans l'ordre dans lequel vous sélectionnez les méthodes :

- **Local** Le nom et le mot de passe stockés localement de l'utilisateur sont utilisés pour l'authentification. Étant donné que la méthode locale n'expire pas, si vous sélectionnez cette option comme première méthode, aucune autre méthode

n'est essayée, même si vous avez spécifié plusieurs méthodes. Il s'agit de la sélection par défaut pour la méthode 1.

- Activer. Le mot de passe d'exécution privilégié est utilisé pour l'authentification.
- Ligne Le mot de passe de ligne est utilisé pour l'authentification.
- Aucun : L'utilisateur est autorisé à y accéder sans authentification.
- Radius Le nom et le mot de passe de l'utilisateur sont authentifiés à l'aide du serveur RADIUS au lieu du serveur local.
- TACACS+ Le nom et le mot de passe de l'utilisateur sont authentifiés à l'aide du serveur TACACS au lieu du serveur local.

8. Dans les menus des colonnes **2, 3, 4, 5** et **6**, sélectionnez les méthodes d'authentification, le cas échéant, qui doivent être utilisées dans la liste de connexion d'authentification sélectionnée.

Si une méthode précédente expire, la méthode suivante est utilisée. Par exemple, la méthode d'authentification sélectionnée dans la colonne **2** est essayée après la méthode d'authentification sélectionnée dans la colonne **1** à l'étape précédente. De même, la méthode d'authentification que vous sélectionnez dans la colonne **3** est essayée après la méthode d'authentification que vous sélectionnez dans la colonne **2**, et ainsi de suite. Si vous sélectionnez une méthode qui n'expire pas, la méthode suivante n'est pas essayée.

Pour les menus des colonnes 2, 3, 4, 5 et 6, en plus des options décrites à l'étape précédente, vous pouvez également sélectionner **N/A**. Avec l'option N/A (qui est la sélection par défaut), la méthode d'authentification n'est pas utilisée. Cette option n'est pas disponible pour le menu de la colonne 1.

9. Effectuez l'une des opérations suivantes :

- Si vous ajoutez une nouvelle liste, cliquez sur le bouton **Ajouter**.
Les paramètres sont enregistrés. L'entrée est ajoutée au tableau.
- Si vous modifiez une liste existante, cliquez sur le bouton **appliquer**.
Les paramètres sont enregistrés.

10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimer une liste d'authentification de connexion

Vous pouvez supprimer une liste ping personnalisée dont vous n'avez plus besoin. Vous ne pouvez pas supprimer la liste des valeurs par défaut et la liste des réseaux.

Pour supprimer une liste d'authentification de connexion :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.
4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **sécurité > sécurité de gestion > liste d'authentification > liste d'authentification de connexion** .
La page Login Authentication List s'affiche.
6. Cochez la case associée à la liste.
7. Cliquez sur le bouton **Supprimer**.
Les paramètres sont enregistrés. La liste est supprimée.
8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez une liste d'activation d'authentification

Une liste d'activation spécifie les méthodes d'authentification permettant de valider l'accès privilégié à l'EXEC dans l'interface de ligne de commande. Une liste d'activation peut s'appliquer aux utilisateurs qui accèdent à la CLI du commutateur par l'une des méthodes suivantes :

- SSH (Secure Shell) Pour plus d'informations sur la sélection d'une liste d'activation pour l'accès SSH, reportez-vous à [Accès de gestion SSH](#) à la page 875 la section .
- Telnet Pour plus d'informations sur la sélection d'une liste d'activation pour l'accès Telnet, reportez-vous à la section [Accès à la gestion Telnet](#) à la page 883.
- Port console Pour plus d'informations sur la sélection d'une liste d'activation pour l'accès au port de console, reportez-vous à [Accès à la gestion des ports de console](#) à la page 887 la section .

Deux listes par défaut sont présentes : enableList et enableNetList. Vous ne pouvez pas supprimer ces listes.

Les utilisateurs préconfigurés (admin et guest) sont affectés à la enableList jusqu'à ce que vous sélectionniez spécifiquement une autre liste.

Tous les utilisateurs nouvellement ajoutés sont également affectés à la enableList jusqu'à ce que vous sélectionniez spécifiquement une autre liste.

Pour configurer une liste d'activation d'authentification :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > gestion de la sécurité > liste d'authentification > Activer la liste d'authentification**.

La page Activer la liste d'authentification s'affiche.

6. Effectuez l'une des opérations suivantes :

- **Créer une nouvelle liste** : Dans le champ nom de la liste, spécifiez un nom. Le nom peut comporter jusqu'à 15 caractères et est sensible à la casse.
- **Modifier une liste existante** : Cochez la case associée à la liste.

7. Dans le menu de la colonne **1**, sélectionnez la méthode d'authentification à utiliser en premier dans la liste de connexion d'authentification sélectionnée.

Si vous sélectionnez une méthode qui n'expire pas comme première méthode, telle que locale, aucune autre méthode n'est essayée, même si vous avez spécifié plusieurs méthodes. L'authentification de l'utilisateur se produit dans l'ordre dans lequel vous sélectionnez les méthodes :

- Activer. Le mot de passe d'exécution privilégié est utilisé pour l'authentification.
- Ligne Le mot de passe de ligne est utilisé pour l'authentification.
- Aucun : L'utilisateur est autorisé à y accéder sans authentification.
- Radius Le nom et le mot de passe de l'utilisateur sont authentifiés à l'aide du serveur RADIUS au lieu du serveur local.
- TACACS+ Le nom et le mot de passe de l'utilisateur sont authentifiés à l'aide du serveur TACACS au lieu du serveur local.
- Refuser L'accès est toujours refusé à l'utilisateur.

8. Dans les menus des colonnes **2, 3, 4 et 5**, sélectionnez les méthodes d'authentification, le cas échéant, à utiliser dans la liste de connexion d'authentification sélectionnée.

Si une méthode précédente expire, la méthode suivante est utilisée. Par exemple, la méthode d'authentification sélectionnée dans la colonne **2** est essayée après la méthode d'authentification sélectionnée dans la colonne **1** à l'étape précédente. De même, la méthode d'authentification que vous sélectionnez dans la colonne **3** est essayée après la méthode d'authentification que vous sélectionnez dans la colonne **2**, et ainsi de suite. Si vous sélectionnez une méthode qui n'expire pas, la méthode suivante n'est pas essayée.

Pour les menus des colonnes 2, 3, 4 et 5, en plus des options décrites à l'étape précédente, vous pouvez également sélectionner **N/A**. Avec l'option N/A (qui est la sélection par défaut), la méthode d'authentification n'est pas utilisée. Cette option n'est pas disponible pour le menu de la colonne 1.

9. Effectuez l'une des opérations suivantes :

- Si vous ajoutez une nouvelle liste, cliquez sur le bouton **Ajouter**.
Les paramètres sont enregistrés. L'entrée est ajoutée au tableau.
- Si vous modifiez une liste existante, cliquez sur le bouton **appliquer**.
Les paramètres sont enregistrés.

10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimez une liste d'activation d'authentification

Vous pouvez supprimer une liste ping personnalisée dont vous n'avez plus besoin. Vous ne pouvez pas supprimer enableList et enableNetList.

Pour supprimer une liste d'activation d'authentification :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > gestion de la sécurité > liste d'authentification > Activer la liste d'authentification**.

La page Activer la liste d'authentification s'affiche.

6. Cochez la case associée à la liste.

7. Cliquez sur le bouton **Supprimer**.

Les paramètres sont enregistrés. La liste est supprimée.

Configurez la liste d'authentification Dot1x.

Vous pouvez configurer la liste d'authentification dot1x, qui spécifie les méthodes d'authentification permettant de valider l'accès au port pour les utilisateurs associés à la liste dot1x. Une seule liste dot1x existe. Pour cette liste, vous ne pouvez sélectionner qu'une seule méthode d'accès. Par défaut, l'accès aux ports ne nécessite pas d'authentification, il n'existe donc aucune méthode d'accès par défaut.

Pour configurer la liste d'authentification dot1x :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > sécurité de gestion > liste d'authentification > liste d'authentification Dot1x**.

La page liste d'authentification Dot1x s'affiche.

6. Cochez la case de la liste dot1x.

7. Sélectionnez la méthode d'authentification à utiliser :

- **IAS** : L'ID et le mot de passe de l'utilisateur dans la base de données du serveur d'authentification interne (IAS) sont utilisés pour l'authentification.
- **Aucun** : L'utilisateur est autorisé à y accéder sans authentification.
- **Radius** Le nom et le mot de passe de l'utilisateur sont authentifiés à l'aide du serveur RADIUS au lieu du serveur local.

8. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez la liste d'authentification HTTP

Vous pouvez configurer la liste d'authentification HTTP, qui spécifie les méthodes d'authentification pour valider l'accès au commutateur ou au port via HTTP, par exemple, via une session de navigateur Web. Il n'existe qu'une seule liste d'authentification HTTP qui, par défaut, utilise l'authentification locale.

Pour configurer la liste d'authentification HTTP :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > sécurité de gestion > liste d'authentification > liste d'authentification HTTP**.

La page liste d'authentification HTTP s'affiche.

6. Cochez la case de la liste HTTP.

7. Dans le menu de la colonne **1**, sélectionnez la méthode d'authentification à utiliser en premier dans la liste de connexion d'authentification sélectionnée.

Si vous sélectionnez une méthode qui n'expire pas comme première méthode, telle que locale, aucune autre méthode n'est essayée, même si vous avez spécifié plusieurs méthodes. L'authentification de l'utilisateur se produit dans l'ordre dans lequel vous sélectionnez les méthodes :

- Local Le nom et le mot de passe stockés localement de l'utilisateur sont utilisés pour l'authentification. Étant donné que la méthode locale n'expire pas, si vous sélectionnez cette option comme première méthode, aucune autre méthode n'est essayée, même si vous avez spécifié plusieurs méthodes. Il s'agit de la sélection par défaut pour la méthode 1.
- Aucun : L'utilisateur est autorisé à y accéder sans authentification.

- Radius Le nom et le mot de passe de l'utilisateur sont authentifiés à l'aide du serveur RADIUS au lieu du serveur local.
 - TACACS+ Le nom et le mot de passe de l'utilisateur sont authentifiés à l'aide du serveur TACACS au lieu du serveur local.
8. Dans les menus des colonnes **2**, **3** et **4**, sélectionnez les méthodes d'authentification, le cas échéant, à utiliser dans la liste de connexion d'authentification sélectionnée.
- Si une méthode précédente expire, la méthode suivante est utilisée. Par exemple, la méthode d'authentification sélectionnée dans la colonne **2** est essayée après la méthode d'authentification sélectionnée dans la colonne **1** à l'étape précédente. De même, la méthode d'authentification que vous sélectionnez dans la colonne **3** est essayée après la méthode d'authentification que vous sélectionnez dans la colonne **2**, et ainsi de suite. Si vous sélectionnez une méthode qui n'expire pas, la méthode suivante n'est pas essayée.
9. Cliquez sur le bouton **Apply** (Appliquer).
- Les paramètres sont enregistrés.
10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez la liste d'authentification HTTPS

Vous pouvez configurer la liste d'authentification HTTPS, qui spécifie les méthodes d'authentification pour valider l'accès au commutateur ou au port via HTTP sécurisé (HTTPS), par exemple, via une session de navigateur Web. Il n'existe qu'une seule liste d'authentification HTTPS qui, par défaut, utilise l'authentification locale.

Pour configurer la liste d'authentification HTTPS :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > sécurité de gestion > liste d'authentification > liste d'authentification HTTPS**.

La page liste d'authentification HTTPS s'affiche.

6. Cochez la case de la liste HTTPS.

7. Dans le menu de la colonne **1**, sélectionnez la méthode d'authentification à utiliser en premier dans la liste de connexion d'authentification sélectionnée.

Si vous sélectionnez une méthode qui n'expire pas comme première méthode, telle que locale, aucune autre méthode n'est essayée, même si vous avez spécifié plusieurs méthodes. L'authentification de l'utilisateur se produit dans l'ordre dans lequel vous sélectionnez les méthodes :

- Local Le nom et le mot de passe stockés localement de l'utilisateur sont utilisés pour l'authentification. Étant donné que la méthode locale n'expire pas, si vous sélectionnez cette option comme première méthode, aucune autre méthode n'est essayée, même si vous avez spécifié plusieurs méthodes. Il s'agit de la sélection par défaut pour la méthode 1.
- Aucun : L'utilisateur est autorisé à y accéder sans authentification.
- Radius Le nom et le mot de passe de l'utilisateur sont authentifiés à l'aide du serveur RADIUS au lieu du serveur local.
- TACACS+ Le nom et le mot de passe de l'utilisateur sont authentifiés à l'aide du serveur TACACS au lieu du serveur local.

8. Dans les menus des colonnes **2, 3 et 4**, sélectionnez les méthodes d'authentification, le cas échéant, à utiliser dans la liste de connexion d'authentification sélectionnée.

Si une méthode précédente expire, la méthode suivante est utilisée. Par exemple, la méthode d'authentification sélectionnée dans la colonne **2** est essayée après la méthode d'authentification sélectionnée dans la colonne **1** à l'étape précédente. De même, la méthode d'authentification que vous sélectionnez dans la colonne **3**

est essayée après la méthode d'authentification que vous sélectionnez dans la colonne **2**, et ainsi de suite. Si vous sélectionnez une méthode qui n'expire pas, la méthode suivante n'est pas essayée.

9. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Sessions de connexion en cours

Vous pouvez afficher des informations sur les sessions de connexion Telnet, série, SSH, HTTP ou HTTPS actuelles sur le commutateur.

Pour afficher les sessions de connexion en cours :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur principale à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > gestion de la sécurité > sessions de connexion**.

La page sessions de connexion s'affiche.

Le tableau suivant décrit les champs affichés dans le tableau.

Table 165 : session de connexion.

Champ	Description
ID (Identifiant)	Identifie l'ID de cette ligne
Nom d'utilisateur	Nom de l'utilisateur pour lequel la session est ouverte
Connexion à partir de	Adresse IP de l'ordinateur à partir duquel l'utilisateur est connecté
Temps d'inactivité :	Durée de la session inactive, le cas échéant
Durée de la session	Durée totale de la session
Type de session	Le type de session : Telnet, Serial, SSH, HTTP ou HTTPS

Accès de gestion HHTTP et HTTPS

Vous pouvez configurer l'accès HTTP et HTTP sécurisé (HTTPS) à l'interface de gestion du commutateur.

Pour configurer les paramètres d'accès HTTP :

Vous pouvez configurer les paramètres d'accès HTTP sur le commutateur. Si vous accédez à l'interface utilisateur principale du commutateur, HTTP est la méthode d'accès par défaut.

Pour configurer les paramètres d'accès HTTP :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > accès > HTTP > Configuration HTTP**.

L'écran HTTP Configuration (Configuration IP) s'affiche.

6. Sélectionnez le bouton radio désactiver ou Activer le mode HTTP.

- Désactiver : Vous ne pouvez pas accéder à l'interface utilisateur principale du commutateur à partir d'une session HTTP via un navigateur Web.
- Activer. Vous pouvez accéder à l'interface utilisateur principale du commutateur à partir d'une session HTTP via un navigateur Web. Il s'agit de l'option par défaut.

7. Dans le champ **Port HTTP**, entrez le numéro de port HTTP.

La plage valide est de 80 et de 1025 à 65535. Le numéro de port par défaut est 80.

8. Dans le champ **HTTP session Soft Timeout (minutes)**, spécifiez le nombre de minutes pendant lesquelles une session HTTP peut être inactive avant qu'un délai ne se produise.

La valeur doit être comprise entre 0 et 60 minutes. La valeur par défaut est 15 minutes.

Une fois la session inactive et expirée, vous êtes automatiquement déconnecté et vous devez saisir à nouveau le mot de passe pour accéder à l'interface utilisateur principale. Une valeur de zéro signifie que la session n'expire pas.

9. Dans le champ **HTTP session Hard Timeout (hours)**, spécifiez le délai d'expiration **Hard** pour les sessions HTTP.

Ce délai n'est pas affecté par le niveau d'activité de la session. La valeur doit être comprise entre 0 et 168 heures. Une valeur de zéro signifie que la session n'expire pas. La valeur par défaut est 24 heures.

10. Dans le champ **nombre maximal de sessions HTTP**, spécifiez le nombre maximal de sessions HTTP pouvant exister simultanément.

Le numéro de port doit être compris entre 0 et 16. La valeur par défaut est 16.

11. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

Le champ liste d'authentification affiche HttpList, qui est la liste par défaut pour l'accès HTTP.

12. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez les paramètres d'accès HTTPS

HTTP sécurisé (HTTPS) permet la transmission de HTTP via une connexion SSL (Secure Sockets Layer) ou TLS (transport Layer Security) chiffrée. Lorsque vous gérez le commutateur sur l'interface utilisateur de l'appareil, HTTPS peut vous aider à garantir que la communication entre le système de gestion et le commutateur est protégée contre les écoutes clandestines et les attaques d'interception.

Pour configurer les paramètres d'accès HTTPS :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > accès > HTTPS > Configuration HTTPS**.

L'écran HTTPS Configuration (Configuration IP) s'affiche.

6. Sélectionnez le bouton radio désactiver ou Activer le mode EEE.

- Désactiver : Vous ne pouvez pas accéder à l'interface utilisateur principale du commutateur à partir d'une session HTTPS via un navigateur Web.

❗ Remarque: Vous pouvez télécharger des certificats SSL uniquement lorsque HTTPS est désactivé.

- Activer. Vous pouvez accéder à l'interface utilisateur principale du commutateur à partir d'une session HTTPS via un navigateur Web. Il s'agit de l'option par défaut.

Le champ État opérationnel indique si HTTPS est activé ou désactivé sur le plan opérationnel. Par exemple, si tous les certificats expirent, HTTPS est désactivé sur le plan opérationnel.

Le champ version TLS affiche la version TLS, qui est toujours 1,2.

7. Dans le champ **Port HTTPS**, spécifiez le numéro de port HTTPS.

La plage valide est comprise entre 1025 et 65535 caractères. Le numéro de port par défaut est 443.

8. Dans le champ **HTTPS session Soft Timeout (minutes)**, spécifiez le nombre de minutes pendant lesquelles une session HTTPS peut être inactive avant qu'un délai ne se produise.

La valeur doit être comprise entre 0 et 60 minutes. La valeur par défaut est 15 minutes.

Une fois la session inactive et expirée, vous êtes automatiquement déconnecté et vous devez saisir à nouveau le mot de passe pour accéder à l'interface utilisateur principale. Une valeur de zéro signifie que la session n'expire pas.

9. Dans le champ **HTTPS session Hard Timeout (hours)**, spécifiez le délai d'expiration **Hard** pour les sessions HTTPS.

Ce délai n'est pas affecté par le niveau d'activité de la session. La valeur doit être comprise entre 0 et 168 heures. Une valeur de zéro signifie que la session n'expire pas. La valeur par défaut est 24 heures.

10. Dans le champ **nombre maximal de sessions HTTPS**, spécifiez le nombre maximal de sessions HTTPS pouvant exister simultanément.

Le numéro de port doit être compris entre 0 et 16. La valeur par défaut est 16.

11. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

Le champ version TLS affiche 1,2, qui est la version par défaut du commutateur.

Le champ liste d'authentification affiche HttpsList, qui est la liste par défaut pour l'accès HTTPS.

12. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Message de sécurité du navigateur avec accès HTTPS

Après avoir activé l'accès HTTPS et tenté d'accéder à l'interface utilisateur de l'appareil, votre navigateur peut afficher un avertissement de sécurité en raison du certificat auto-signé sur le commutateur. Il s'agit d'un comportement attendu. Vous pouvez poursuivre ou ajouter une exception pour l'avertissement de sécurité.

Pour continuer avec un avertissement de sécurité ou ajouter une exception pour un avertissement de sécurité :

- Google Chrome Cliquez sur le lien **AVANCÉ**. Cliquez ensuite sur le lien **Proceed to x.x.x.x (non sécurisé)**, dans lequel x.x.x.x représente le nom de domaine ou l'adresse IP du périphérique.
- Apple Safari Cliquez sur le bouton **Afficher les détails**. Cliquez ensuite sur le lien **visiter ce site Web**. Si une fenêtre contextuelle d'avertissement s'affiche, cliquez sur le bouton **visiter le site Web**. Si une autre fenêtre contextuelle s'affiche pour vous permettre de confirmer les modifications apportées aux paramètres de confiance de votre certificat, entrez votre nom d'utilisateur Mac et votre mot de passe, puis cliquez sur le bouton **mettre à jour les paramètres**.
- Mozilla Firefox Cliquez sur le bouton **AVANCÉ**. Cliquez ensuite sur le bouton **Ajouter une exception**. Dans la fenêtre contextuelle qui s'affiche, cliquez sur le bouton **confirmer l'exception de sécurité**.
- Microsoft Edge Sélectionnez **Détails > aller à la page Web**.
- Microsoft Internet Explorer Cliquez sur le lien **continuer vers ce site Web (non recommandé)**.

❗ **Remarque:** Pour plus d'informations sur l'installation d'un certificat de sécurité spécifique sur le commutateur, reportez-vous aux sections [Gérer les certificats pour l'accès HTTPS](#), à la page 867 et [Téléchargez et installez un fichier de certificat de sécurité SSL sur le commutateur](#) à la page 1161.

Gérer les certificats pour l'accès HTTPS .

Vous pouvez gérer les certificats pour l'accès HTTPS. Le commutateur prend en charge deux certificats, dont l'un peut être le certificat actif.

Vous pouvez générer un certificat sur le commutateur ou transférer un certificat d'un serveur vers le commutateur.

Afficher l'état des certificats SSL

Le commutateur peut contenir des certificats auto-générés que vous avez ajoutés et des certificats que vous avez transférés au commutateur.

Pour afficher l'état des certificats SSL :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > accès > HTTPS > gestion des certificats**.

La page gestion des certificats s'affiche.

6. Dans le menu **numéro de certificat**, sélectionnez le certificat, c'est-à-dire **1** ou **2**.

❗ Remarque: Un certificat que vous transférez (téléchargez) vers le commutateur reçoit le numéro 1.

Le champ certificat présent s'affiche si le certificat sélectionné est présent sur le commutateur.

Le champ certificat expiré s'affiche si le certificat sélectionné a expiré.

La section État du certificat affiche les informations suivantes pour tous les certificats du commutateur :

- Certificat actif : Certificats actifs sur le commutateur. Si HTTPS est désactivé, aucun s'affiche. Sinon, les numéros de certificat sont affichés.
- Certificat(s) expiré(s) : Tous les certificats expirés sur le commutateur.

Générez un certificat SSL

Vous pouvez générer jusqu'à deux certificats SSL auto-signés pour la communication HTTPS.

❗ Remarque: Avant de pouvoir générer un certificat, vous devez désactiver HTTPS (voir [Configurez les paramètres d'accès HTTPS](#) à la page 865) et vous reconnecter à l'interface utilisateur principale via une session HTTP. Après avoir généré le certificat, vous pouvez réactiver HTTPS et vous reconnecter à l'interface utilisateur principale via une session HTTPS.

Pour générer un certificat SSL :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > accès > HTTPS > gestion des certificats**.

La page gestion des certificats s'affiche.

6. Dans le menu **numéro de certificat**, sélectionnez le certificat, c'est-à-dire **1** ou **2**.

Votre sélection détermine si le premier ou le deuxième certificat est généré.

7. Sélectionnez le bouton radio **générer des certificats**.

8. Cliquez sur le bouton **Apply** (Appliquer).

Le commutateur génère un certificat SSL.

Le champ État de génération de certificat indique que le commutateur est en train de générer un certificat.

9. Cliquez sur le bouton **Actualiser**.

Le champ certificat présent affiche Oui, indiquant que le certificat est présent.

10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Activer un certificat

Après avoir ajouté un certificat SSL auto-généré ou transféré (téléchargement) et signé par une autorité de certification externe au commutateur, vous pouvez activer le certificat.

Pour activer un certificat :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > accès > HTTPS > gestion des certificats**.

La page gestion des certificats s'affiche.

6. Dans le menu **numéro de certificat**, sélectionnez le certificat, c'est-à-dire **1** ou **2**.

Votre sélection détermine si le premier ou le deuxième certificat est activé.

7. Sélectionnez le bouton radio **Activer le certificat**.

8. Cliquez sur le bouton **Apply** (Appliquer).

Vos paramètres sont enregistrés et le certificat est maintenant actif.

9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimer un certificat SSL

❗ Remarque: Avant de pouvoir supprimer un certificat, vous devez désactiver HTTPS (voir [Configurez les paramètres d'accès HTTPS](#) à la page 865) et vous reconnecter à l'interface utilisateur principale via une session HTTP. Après avoir supprimé le certificat, vous pouvez réactiver HTTPS et vous reconnecter à l'interface utilisateur principale via une session HTTPS.

Pour supprimer un certificat SSL :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **sécurité > accès > HTTPS > gestion des certificats**.
Le champ certificat présent affiche Oui.
6. Dans le menu **numéro de certificat**, sélectionnez le certificat, c'est-à-dire **1** ou **2**.
Votre sélection détermine si le premier ou le deuxième certificat est supprimé.
7. Sélectionnez le bouton radio **Supprimer les certificats**.
8. Cliquez sur le bouton **Apply** (Appliquer).
Le certificat est supprimé.

Transférer un certificat HTTPS existant d'un serveur vers le commutateur

Vous pouvez transférer un fichier de certificat d'un serveur sécurisé vers le commutateur. Un certificat que vous transférez vers le commutateur reçoit le numéro 1.

❗ Remarque: Pour plus d'informations sur le téléchargement et l'installation d'un certificat SSL sur une session HTTP, reportez-vous à la section [Téléchargez et installez un fichier de certificat de sécurité SSL sur le commutateur](#) à la page 1161.

Pour que le commutateur accepte les connexions HTTPS d'un terminal, il nécessite un certificat de clé publique. Vous pouvez générer un certificat en externe (par exemple, hors ligne) ou obtenir un certificat signé par une autorité de certification et transférer informatique vers le commutateur.

Avant de transférer un fichier d'un serveur TFTP vers le commutateur, les conditions suivantes doivent être remplies :

- Le fichier que vous transférez à partir d'un serveur TFTP se trouve sur le serveur dans le répertoire approprié.
- Le format du fichier est correct.
- Le commutateur contient un chemin d'accès au serveur.

❗ Remarque: Avant de pouvoir transférer un certificat, vous devez désactiver HTTPS (voir [Configurez les paramètres d'accès HTTPS](#) à la page 865) et vous reconnecter à l'interface utilisateur principale via une session HTTP. Après avoir transféré le certificat, vous pouvez réactiver HTTPS et vous reconnecter à l'interface utilisateur principale via une session HTTPS.

Pour transférer un certificat HTTPS vers le commutateur :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > accès > HTTPS > Téléchargement de certificat**.

La page mise à jour du certificat s'affiche.

6. Dans le menu **type de fichier**, sélectionnez le type de certificat SSL à télécharger :

- **Fichier PEM de certificat racine sécurisé SSL** : Un fichier de certificat racine sécurisé SSL (codé PEM).
 - **Fichier PEM de certificat de serveur SSL** : Fichier de certificat de serveur SSL (encodé PEM)
 - **SSL DH 1024 fichier PEM de paramètre de cryptage** : Fichier de paramètres de cryptage SSL Diffie-Hellman 1024 bits (codé PEM)
 - **SSL DH 2048 fichier PEM de paramètre de cryptage** : Fichier de paramètres de cryptage SSL Diffie-Hellman 2048 bits (codé PEM)
7. Dans le menu **Transfer mode**, spécifiez le protocole à utiliser pour transférer le fichier vers le serveur :
- TFTP Protocole Trivial File Transfer.
 - SFTP Protocole de transfert de fichiers sécurisé.
 - **SCP**: Protocole de copie sécurisé.
8. Dans le menu **type d'adresse du serveur**, sélectionnez **IPv4**, **IPv6** ou **DNS** pour indiquer le format du champ IP du serveur TFTP.
La valeur par défaut est IPv4.
9. Dans le champ **adresse du serveur**, spécifiez l'adresse ou le nom d'hôte du serveur.
L'adresse peut être une adresse IP au format IPv4 ou IPv6 standard ou un nom d'hôte.
Le nom d'hôte doit commencer par une lettre de l'alphabet.
10. Dans le champ **chemin du fichier distant**, entrez le chemin du fichier à télécharger.
Vous pouvez entrer jusqu'à 96 caractères. La valeur par défaut est vide.
11. Dans le champ **nom du fichier distant**, entrez le nom du fichier à télécharger sur le serveur TFTP.
Vous pouvez entrer jusqu'à 32 caractères. La valeur par défaut est vide.
12. Si vous sélectionnez **SFTP** ou **SCP** dans le menu **Transfer mode**, spécifiez les paramètres suivants :
- Nom d'utilisateur : Spécifiez le nom d'utilisateur pour la connexion à distance au serveur.
 - Nouveau mot de passe : Spécifiez le mot de passe pour la connexion à distance au serveur.
13. Cliquez sur le bouton **Apply** (Appliquer).
Le transfert de fichier démarre.
Un message d'état s'affiche pendant le transfert et une fois le transfert terminé avec succès.

Une fois le transfert de fichier terminé, le certificat reçoit le numéro 1.

14. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Accès de gestion SSH

Vous pouvez afficher et modifier les paramètres du serveur Secure Shell (SSH) sur le commutateur. SSH est un protocole réseau qui permet d'accéder à l'interface de gestion CLI à l'aide d'un client SSH sur un système d'administration distant. SSH est une méthode d'accès plus sécurisée que Telnet car informatique crypte les communications entre le système d'administration et le périphérique. Vous pouvez télécharger ou générer des clés d'hôte SSH pour une gestion sécurisée basée sur la CLI.

Configurez les paramètres d'accès SSH globaux

Vous pouvez configurer les paramètres d'accès SSH globaux.

Pour configurer les paramètres SSH :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **sécurité > accès > SSH > Configuration SSH**.
L'écran SSH Configuration (Configuration IP) s'affiche.
6. Sélectionnez le bouton radio **désactiver** ou **Activer** le mode Admin SSH.
Cette sélection active ou désactive le mode d'administration global SSH. Lorsque cette option est activée, vous pouvez accéder au commutateur à l'aide d'un client SSH sur un système distant. La valeur par défaut est désactiver.
7. Dans le champ **délai de session SSH**, spécifiez le délai d'inactivité des sessions SSH vers le commutateur.
Si une session SSH est inactive et que le délai d'expiration est dépassé, la session est interrompue. La plage est de 1 à 160 secondes. La valeur par défaut est 5 minutes.
8. Dans le champ **nombre maximal de sessions SSH**, spécifiez le nombre maximal de sessions SSH pouvant être effectuées simultanément sur le commutateur.
La plage est de 0 à 5. La valeur par défaut est de 5 sessions.
9. Dans le menu **liste d'authentification**, sélectionnez une liste d'authentification de connexion.
Cette liste est utilisée pour authentifier les utilisateurs qui tentent de se connecter au commutateur. La liste par défaut est NetworkList. Pour plus d'informations sur les listes d'authentification de connexion, reportez-vous à la section [Configurez une liste d'authentification de connexion](#) à la page 850.
10. Dans le menu **Activer la liste d'authentification**, sélectionnez une liste Activer l'authentification.
Cette liste est utilisée pour authentifier les utilisateurs qui tentent d'obtenir un accès privilégié à l'EXEC. La liste par défaut est enableList. Pour plus d'informations sur l'activation des listes d'authentification, reportez-vous à la section [Configurez une liste d'activation d'authentification](#) à la page 854.
11. Dans le champ **Port SSH**, spécifiez le port pour l'accès SSH.
La plage est de 1 à 65535. Le numéro de port par défaut est 22.
12. Sélectionnez le bouton radio **désactiver** ou **Activer** le mode d'authentification par clé publique SSH.
Cette sélection active ou désactive le mode d'authentification par clé publique SSH. Lorsque cette option est activée, vous pouvez utiliser une clé publique sécurisée plutôt qu'un mot de passe pour accéder au commutateur via une session SSH. La valeur par défaut est désactiver.
13. Sélectionnez le bouton radio **désactiver** ou **Activer** le mode Admin du serveur SCP.

Cette sélection active ou désactive les transferts de fichiers sur un serveur SCP (Secure Copy Protocol). La valeur par défaut est désactiver.

14. Dans le champ **nombre maximal de tentatives d'authentification SSH**, spécifiez le nombre de tentatives d'authentification d'un client SSH par le commutateur après l'échec de l'authentification initiale.

La plage est comprise entre 0 et 5. Le numéro par défaut est 3.

15. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

16. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 166 : Informations de configuration SSH

Champ	Description
Version SSH	Le commutateur peut accepter les connexions d'un client SSH à l'aide du niveau de protocole 2 pour SSH (SSH-2). Le niveau de protocole 2 pour SSH est activé par défaut.
Nombre actuel de sessions SSH	Nombre de sessions SSH actives entre les clients SSH distants et le commutateur.
Touches présentes	S'affiche si l'une des touches suivantes ou les deux (le cas échéant) sont présentes sur l'appareil : • Un fichier de clé SSH-2 Rivest-Shamir-Adelman (RSA) (codé PEM). • Un fichier de clé SSH-2 Digital signature Algorithm (DSA) (codé PEM). Si aucune touche n'est présente, non s'affiche.
Nombre maximal de tentatives d'authentification SSH	Nombre de tentatives d'authentification du client SSH par le commutateur. Par défaut, ce nombre est 4.

Gérer les clés RSA, DSA et ECDSA pour l'accès SSH

Vous pouvez gérer Rivest-Shamir-Adelman (RSA) et diverses versions des clés DSA (Digital signature Algorithm) pour l'accès SSH au commutateur.

Générez une clé RSA, DSA ou ECDSA

Le commutateur prend en charge les clés suivantes utilisées pour l'accès SSH :

- **RSA** : Rivest-Shamir-Adleman (RSA), qui est un algorithme largement supporté.
- **DSA** : Digital signature Algorithm (DSA), qui est un algorithme sécurisé pour l'authentification mais pas pour le chiffrement.
- **ECDSA** : Elliptic Curve Digital signature Algorithm (ECDSA), un algorithme plus récent et très sécurisé qui n'est pas encore largement pris en charge.

❗ **Remarque:** Pour générer un fichier de clé SSH, SSH doit être désactivé (voir [Configurez les paramètres d'accès SSH globaux](#) à la page 875).

Pour générer une clé RSA, DSA ou ECDSA :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > accès > SSH > gestion des clés d'hôte**.

La page gestion des clés d'hôte s'affiche.

Le champ clés présentes indique si un certificat est présent sur le commutateur.

6. Effectuez une ou plusieurs des opérations suivantes :

- **Clé RSA** : Dans la section gestion des clés RSA, dans le champ **longueur de clé**, spécifiez une longueur de clé et sélectionnez le bouton radio **générer des clés RSA**.

Les longueurs de clé prises en charge pour RSA sont 1024, 2048 et 3072. Le numéro par défaut est 1024.

- **Clé DSA** : Dans la section gestion des clés DSA, sélectionnez le bouton radio **générer des clés DSA**.
- **Clé ECDSA** : Dans la section gestion des clés ECDSA, dans le champ **longueur de clé**, spécifiez une longueur de clé et sélectionnez le bouton radio **générer des clés ECDSA**.

Les longueurs de clé prises en charge pour ECDSA sont 256, 384 et 521. Le numéro par défaut est 256.

7. Cliquez sur le bouton **Apply** (Appliquer).

Le commutateur génère une clé. Le champ génération de clé en cours affiche des informations de progression.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 167 : Informations sur l'état de la clé hôte

Champ	Description
Touches présentes	Affiche les touches présentes sur le commutateur (le cas échéant) : RSA, DSA, ECDSA ou aucun.
Génération de clé en cours	Affiche la clé générée (le cas échéant) : RSA, DSA, ECDSA ou aucun.

Supprimez une clé RSA, DSA ou ECDSA

❗ Remarque : Pour supprimer un fichier de clé SSH, SSH doit être désactivé (voir [Configurez les paramètres d'accès SSH globaux](#) à la page 875).

Pour supprimer une clé RSA, DSA ou ECDSA :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > accès > SSH > gestion des clés d'hôte** .

La page gestion des clés d'hôte s'affiche.

Le champ clés présentes affiche Oui.

6. Effectuez une ou plusieurs des opérations suivantes :

- **Clé RSA** : Dans la section gestion des clés RSA, sélectionnez le bouton radio **Supprimer les clés RSA**.
- **Clé DSA** : Dans la section gestion des clés DSA, sélectionnez le bouton radio **Supprimer les clés DSA**.
- **Clé ECDSA** : Dans la section gestion des clés ECDSA, sélectionnez le bouton radio **Supprimer les clés ECDSA**.

7. Cliquez sur le bouton **Apply** (Appliquer).

Les clés sont retirées.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Transférer des clés SSH existantes d'un serveur TFTP vers le commutateur

Vous pouvez transférer un fichier de clé SSH-2 RSA, SSH-2 DSA ou ECDSA Privacy Enhanced mail (PEM) d'un commutateur distant ou d'un ordinateur vers le commutateur.

Avant de transférer un fichier d'un serveur TFTP vers le commutateur, les conditions suivantes doivent être remplies :

- Le fichier que vous transférez à partir d'un serveur TFTP se trouve sur le serveur dans le répertoire approprié.
- Le format du fichier est correct.
- Le commutateur contient un chemin d'accès au serveur.

❗ Remarque: Pour télécharger un fichier de clé SSH sur le commutateur, SSH doit être désactivé (voir [Configurez les paramètres d'accès SSH globaux](#) à la page 875).

Pour transférer des clés SSH vers le commutateur :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > accès > SSH > Téléchargement des clés d'hôte** .

La page de téléchargement de clés hôtes s'affiche.

6. Dans le menu **type de fichier**, sélectionnez le type de fichier de clé à télécharger :

- **Fichier PEM de clé RSA SSH-2** : Un fichier de clé SSH-2 Rivest-Shamir-Adelman (RSA) (codé PEM).
 - **Fichier PEM de clé DSA SSH-2** : Un fichier de clé SSH-2 Digital signature Algorithm (DSA) (codé PEM).
 - **Fichier PEM de clé ECDSA** : Fichier de clé ECDSA (Elliptic Curve Digital signature Algorithm) (codé PEM).
7. Dans le menu **Transfer mode**, spécifiez le protocole à utiliser pour transférer le fichier vers le serveur :
 - TFTP Protocole Trivial File Transfer.
 - SFTP Protocole de transfert de fichiers sécurisé.
 - **SCP**: Protocole de copie sécurisé.
 8. Dans le menu **type d'adresse du serveur**, sélectionnez **IPv4**, **IPv6** ou **DNS** pour indiquer le format du champ IP du serveur TFTP.
La valeur par défaut est IPv4.
 9. Dans le champ **IP du serveur**, spécifiez l'adresse ou le nom d'hôte du serveur.
L'adresse peut être une adresse IP au format IPv4 ou IPv6 standard ou un nom d'hôte. Le nom d'hôte doit commencer par une lettre de l'alphabet.
 10. Dans le champ **chemin du fichier distant**, entrez le chemin du fichier à télécharger.
Vous pouvez entrer jusqu'à 96 caractères. La valeur par défaut est vide.
 11. Dans le champ **nom du fichier distant**, entrez le nom du fichier à télécharger sur le serveur TFTP.
Vous pouvez entrer jusqu'à 32 caractères. La valeur par défaut est vide.
 12. Si vous sélectionnez **SFTP** ou **SCP** dans le menu **Transfer mode**, entrez le nom d'utilisateur dans le champ **Username**.
Il s'agit du nom d'utilisateur avec lequel vous accédez au serveur SFTP ou SCP.
 13. Si vous sélectionnez **SFTP** ou **SCP** dans le menu **Transfer mode**, entrez le mot de passe dans le champ **Password**.
Il s'agit du mot de passe requis pour accéder au serveur SFTP ou SCP.
 14. Cliquez sur le bouton **Apply** (Appliquer).
Le transfert de fichier démarre. Un message d'état s'affiche pendant le transfert et une fois le transfert terminé avec succès.
 15. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Accès à la gestion Telnet

Vous pouvez configurer les listes d'authentification Telnet et gérer Telnet sortant et entrant.

Sélectionnez listes d'authentification Telnet

Vous pouvez sélectionner une liste d'authentification de connexion et une liste d'activation d'authentification :

- **Liste d'authentification de connexion** : La liste de connexion spécifie les méthodes d'authentification utilisées pour valider l'accès au commutateur ou au port pour les utilisateurs associés à la liste. Pour plus d'informations, consultez [Configurez une liste d'authentification de connexion](#) à la page 850.
- **Activer la liste d'authentification** : La liste Enable spécifie les méthodes d'authentification utilisées pour valider l'accès privilégié des utilisateurs associés à la liste. Pour plus d'informations, consultez [Configurez une liste d'activation d'authentification](#) à la page 854.

Pour configurer les listes d'authentification Telnet :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **sécurité > accès > Telnet**.
La page Telnet s'affiche.
6. Dans le menu **liste d'authentification**, sélectionnez la liste d'authentification de connexion à utiliser pour établir une session Telnet.
La valeur par défaut est NetworkList.
7. Dans le menu **Activer la liste d'authentification**, sélectionnez la liste d'activation d'authentification qui doit être utilisée pour accéder au mode d'exécution privilégié dans une session Telnet établie.
La valeur par défaut est enableList.
8. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez les paramètres Telnet entrants

Si vous activez les sessions Telnet entrantes et autorisez l'établissement de nouvelles sessions Telnet, les utilisateurs autorisés peuvent établir de nouvelles sessions Telnet sur le commutateur jusqu'à ce que le nombre maximal de sessions Telnet soit dépassé. Une session Telnet établie reste active jusqu'à ce qu'elle soit terminée ou que le délai d'expiration de la session soit dépassé.

Pour configurer les paramètres Telnet entrants :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > accès > Telnet**.

La page Telnet s'affiche.

6. Dans la section Telnet entrant, configurez les paramètres suivants :

- a. Sélectionnez le bouton radio **désactiver** ou **Activer** le mode Admin du serveur Telnet.

Cette sélection spécifie si le commutateur accepte des sessions Telnet entrantes. Par défaut, le bouton radio Ethernet est sélectionné.

- b. En regard de autoriser de nouvelles sessions Telnet, sélectionnez le bouton radio **désactiver** ou **Activer**.

Cette sélection spécifie si le commutateur accepte de nouvelles sessions Telnet, c'est-à-dire, nouvelles en plus d'une session Telnet en cours. Par défaut, le bouton radio Ethernet est sélectionné. Si vous désactivez cette option, une session établie reste active jusqu'à ce qu'elle soit terminée, après quoi aucune nouvelle session Telnet ne peut être établie.

- c. Dans le champ **délai d'expiration de la session (minutes)**, spécifiez le délai en minutes après lequel une session Telnet inactive se termine automatiquement.

La plage est de 1 à 160 secondes. La valeur par défaut est 5 minutes.

- d. Dans le champ **nombre maximal de sessions**, spécifiez le nombre de sessions Telnet entrantes simultanées autorisées.

Le maximum est 5, qui est également la valeur par défaut.

7. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

Le champ nombre actuel de sessions de la section Telnet entrant affiche le nombre de sessions Telnet entrantes actuelles.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurer les paramètres Telnet sortants

Si vous activez les sessions Telnet sortantes et autorisez l'établissement de nouvelles sessions Telnet, les utilisateurs autorisés peuvent établir de nouvelles sessions Telnet du commutateur vers une autre unité jusqu'à ce que le nombre maximal de sessions Telnet soit dépassé. Une session Telnet établie reste active jusqu'à ce qu'elle soit terminée ou que le délai d'expiration de la session soit dépassé.

Pour configurer les paramètres Telnet sortants :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > accès > Telnet**.

La page Telnet s'affiche.

6. Dans la section Telnet sortant, configurez les paramètres suivants :
 - a. En regard de autoriser de nouvelles sessions Telnet, sélectionnez le bouton radio **désactiver** ou **Activer**.

Cette sélection spécifie si le commutateur autorise *de nouvelles* sessions Telnet sortantes. Par défaut, le bouton radio Ethernet est sélectionné. Si vous désactivez cette option, une session établie reste active jusqu'à ce qu'elle soit terminée.
 - b. Dans le champ **délai d'expiration de la session (minutes)**, spécifiez le délai en minutes après lequel une session Telnet inactive se termine automatiquement.

La plage est de 1 à 160 secondes. La valeur par défaut est 5 minutes.
 - c. Dans le champ **nombre maximal de sessions**, spécifiez le nombre de sessions Telnet sortantes simultanées autorisées.

Le maximum est 5, qui est également la valeur par défaut.
7. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

Le champ nombre actuel de sessions de la section Telnet sortant affiche le nombre de sessions Telnet sortantes actuelles.
8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Accès à la gestion des ports de console

Vous pouvez configurer les paramètres d'une connexion port série (port console) au commutateur.

Pour configurer les paramètres du port de console :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > accès > Port de console**.

La page Port de console s'affiche.

6. Dans le champ **Serial Port Login Timeout (minutes) (délai de connexion au port série (minutes))**, spécifiez le délai en minutes après lequel une connexion de port de console inactive se termine automatiquement.

La plage est de 1 à 160 secondes. La valeur par défaut est 5 minutes. La saisie de 0 désactive le délai d'attente.

7. Dans le menu **débit en bauds (bps)**, sélectionnez le débit en bauds par défaut pour la connexion du port de console.

Vous pouvez choisir entre 1200, 2400, 4800, 9600, 19200, 38400, 57600 et 115200 bauds. La valeur par défaut est 115200 bauds.

8. Dans le menu **liste d'authentification**, sélectionnez une liste d'authentification de connexion.

Cette liste est utilisée pour authentifier les utilisateurs qui tentent de se connecter au commutateur. La valeur par défaut est DefaultList. Pour plus d'informations sur les listes d'authentification de connexion, reportez-vous à la section [Configurez une liste d'authentification de connexion](#) à la page 850.

9. Dans le menu **Activer la liste d'authentification**, sélectionnez une liste Activer l'authentification.

Cette liste est utilisée pour authentifier les utilisateurs qui tentent d'obtenir un accès privilégié à l'EXEC. La liste par défaut est enableList. Pour plus d'informations sur l'activation des listes d'authentification, reportez-vous à la section [Configurez une liste d'activation d'authentification](#) à la page 854.

10. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

11. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 168 : Informations sur le port de console

Champ	Description
Taille des caractères (bits)	Nombre de bits dans un caractère. Ce paramètre est toujours 8.
Contrôle des flux	Indique si le contrôle de flux matériel est activé ou désactivé. Ce paramètre est toujours désactivé.
Bit d'arrêt.	Nombre de bits d'arrêt par caractère. Ce paramètre est toujours 1.
Parité.	Méthode de parité utilisée sur le port de console. Ce paramètre est toujours aucun.

Déni de service

Vous pouvez sélectionner les types d'attaques par déni de service (dos) que le commutateur surveille et bloque.

Pour configurer des paramètres dos individuels :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > accès > Configuration du déni de service**.

La page Configuration du déni de service s'affiche.

6. Sélectionnez les types d'attaques dos que le commutateur doit surveiller et bloquer et configurez les valeurs associées :

- **Déni de service taille d'en-tête TCP min** : Spécifiez la taille d'en-tête TCP minimale autorisée. Si vous sélectionnez le bouton radio **fragment TCP déni de service**, le commutateur supprime le premier fragment TCP avec un paquet de données utiles TCP pour lequel la taille d'en-tête TCP minimale est supérieure à la longueur de données utiles IP moins la taille d'en-tête IP. La taille minimale de l'en-tête TCP est comprise entre 0 et 255. La valeur par défaut est 20.
- **Déni de service ICMPv4**. L'activation de la prévention dos ICMPv4 entraîne l'abandon par le commutateur des paquets ICMPv4 dont le type est ECHO_REQ (ping) et dont la taille est supérieure à la taille de paquet ICMPv4 configurée. Par défaut, cette fonctionnalité est désactivée.
- **Déni de service taille maximale des paquets ICMPv4**. Spécifiez la taille de paquet ICMPv4 maximale autorisée. Si la prévention dos ICMPv4 est activée, le commutateur supprime les paquets ping ICMPv4 dont la taille est supérieure à la valeur configurée. La plage est de 0 à 16376. La valeur par défaut est 512.
- **Déni de service ICMPv6**. L'activation de la prévention dos ICMPv6 entraîne l'abandon par le commutateur des paquets ICMPv6 dont le type est ECHO_REQ (ping) et dont la taille est supérieure à la taille de paquet ICMPv6 configurée. Par défaut, cette fonctionnalité est désactivée.
- **Déni de service taille maximale des paquets ICMPv6**. Spécifiez la taille de paquet ICMPv6 maximale autorisée. Si la prévention dos ICMPv6 est activée, le commutateur supprime les paquets ping ICMPv6 dont la taille est supérieure à la valeur configurée. La plage est de 0 à 16376. La valeur par défaut est 512.

- **Déni de service premier fragment** : L'activation de la prévention dos du premier fragment amène le commutateur à vérifier les options dos sur le premier fragment d'un paquet IP fragmenté. Sinon, le commutateur ignore le premier fragment d'un paquet IP fragmenté. Par défaut, cette fonctionnalité est désactivée.
- **Déni de service ICMP fragment** : L'activation de la prévention dos de service ICMP fragment entraîne l'abandon par le commutateur des paquets fragmentés ICMP. Par défaut, cette fonctionnalité est désactivée.
- **Déni de service SIP=DIP** : L'activation de la prévention dos SIP=DIP entraîne l'abandon par le commutateur des paquets dont l'adresse IP source est égale à l'adresse IP de destination. Par défaut, cette fonctionnalité est désactivée.
- **Déni de service SMAC=DMAC** : L'activation de la prévention dos SMAC=DMAC entraîne l'abandon par le commutateur des paquets dont l'adresse MAC source est égale à l'adresse MAC de destination. Par défaut, cette fonctionnalité est désactivée.
- **Déni de service TCP fin&URG&PSH** : L'activation de la prévention dos TCP fin & URG & PSH entraîne l'abandon par le commutateur des paquets avec les drapeaux TCP fin, URG et PSH définis et le numéro de séquence TCP égal à 0. Par défaut, cette fonctionnalité est désactivée.
- **Drapeau et séquence TCP de déni de service** : L'activation de la prévention dos par drapeau TCP entraîne l'abandon par le commutateur des paquets dont les drapeaux de contrôle TCP sont définis sur 0 et le numéro de séquence TCP sur 0. Par défaut, cette fonctionnalité est désactivée.
- **Fragment TCP de déni de service** : L'activation de la prévention dos de fragment TCP entraîne l'abandon par le commutateur de paquets avec une charge utile TCP pour lesquels la longueur de charge utile IP moins la taille d'en-tête IP est inférieure à la taille d'en-tête TCP minimale autorisée. Par défaut, cette fonctionnalité est désactivée.
- **Décalage TCP de déni de service** : L'activation de la prévention dos de décalage TCP entraîne l'abandon par le commutateur des paquets dont le décalage d'en-tête TCP est défini sur 1. Par défaut, cette fonctionnalité est désactivée.
- **Port TCP de déni de service** : L'activation de la prévention dos de port TCP entraîne l'abandon par le commutateur des paquets pour lesquels le port source TCP est égal au port de destination TCP. Par défaut, cette fonctionnalité est désactivée.
- **Déni de service TCP SYN** : L'activation de la prévention dos TCP SYN entraîne l'abandon par le commutateur des paquets avec l'indicateur TCP SYN défini. Par défaut, cette fonctionnalité est désactivée.
- **Déni de service TCP SYN&fin** : L'activation de la prévention dos TCP SYN et fin entraîne l'abandon par le commutateur des paquets avec les drapeaux TCP SYN et fin définis. Par défaut, cette fonctionnalité est désactivée.

- **Port UDP de déni de service** : L'activation de la prévention dos de port UDP entraîne l'abandon par le commutateur des paquets pour lesquels le port source UDP est égal au port de destination UDP. Par défaut, cette fonctionnalité est désactivée.
- **Mode DROP de balise VLAN0 empilé** : L'activation du mode d'abandon de balise pour VLAN 0 empilé entraîne le transfert ou l'abandon des paquets étiquetés avec VLAN 0 et le transfert ou l'abandon des paquets SNAP. (SNAP est l'acronyme de Stateful Network-Wide abstractions for Packet Processing.) Par défaut, cette fonctionnalité est désactivée.

7. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Profils et règles d'accès de gestion

Le contrôle d'accès vous permet de configurer un profil de contrôle d'accès et de définir des règles pour l'accès à l'interface utilisateur principale, l'accès par des stations SNMP et l'accès client à un serveur TFTP. Nous appelons profil de contrôle d'accès un profil d'accès. Vous pouvez ajouter un profil d'accès unique, que vous pouvez configurer, activer ou désactiver.

 **Attention:** Si vous configurez un profil d'accès de sécurité de manière incorrecte et que vous activez le profil d'accès, vous risquez de ne plus pouvoir accéder à l'interface utilisateur principale du commutateur. Si cette situation se produit, vous devez réinitialiser le commutateur aux paramètres par défaut (voir [Pour rétablir les paramètres par défaut du routeur](#) : à la page 1144).

Ajouter un profil d'accès .

Vous pouvez définir un profil d'accès de sécurité unique auquel vous pouvez associer une configuration de règle d'accès.

Pour ajouter un profil d'accès :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > accès > contrôle d'accès > Configuration du profil d'accès**

La page Configuration du profil d'accès s'affiche.

6. Dans le champ **nom du profil d'accès**, entrez le nom du profil d'accès à ajouter.

La longueur maximale autorisée est de 32 caractères.

7. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés. Par défaut, le profil d'accès est désactivé. Après avoir ajouté des règles, vous pouvez activer le profil d'accès.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Ajoutez une règle au profil d'accès.

Après avoir ajouté le profil d'accès, vous pouvez ajouter une ou plusieurs règles d'accès de sécurité au profil d'accès.

Si vous accédez au commutateur à partir d'un ordinateur, assurez-vous d'ajouter une règle d'autorisation pour le type de service que vous utilisez (par exemple, HTTPS), l'adresse IP de votre ordinateur et le masque de sous-réseau de votre ordinateur.

 **Attention:** Vous devez ajouter une règle d'autorisation pour votre terminal et votre méthode d'accès, sinon vous êtes verrouillé pour accéder au commutateur après avoir activé le profil d'accès. Si cette situation se produit, vous devez réinitialiser le commutateur aux paramètres par défaut (voir [Pour rétablir les paramètres par défaut du routeur](#) : à la page 1144).

Ajoutez une règle au profil d'accès.

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > accès > contrôle d'accès > Configuration des règles d'accès**.

La page Configuration des règles d'accès s'affiche.

6. Dans le menu **type de règle**, sélectionnez **autoriser** ou **refuser** pour autoriser ou refuser l'accès lorsque les règles sélectionnées correspondent.

Une règle autoriser autorise l'accès à partir d'un terminal qui correspond aux critères de la règle. Une règle refuser bloque un terminal qui correspond aux critères de la règle.

7. Dans le menu **type de service**, sélectionnez la méthode d'accès à laquelle la règle est appliquée.

Sauf si vous autorisez une méthode d'accès, la stratégie est restreinte par la méthode d'accès sélectionnée. Les méthodes d'accès possibles sont **any**, **TELNET**, **TFTP**, **HTTP**, **Secure HTTP (SSL)**, **SNMP**, **Secure Telnet (SSH)** et **NTP**.

8. Dans le champ **adresse IP source**, entrez l'adresse IP source d'où provient le trafic de gestion.
9. Dans le champ **masque**, spécifiez le masque de sous-réseau d'où provient le trafic de gestion.
10. Dans le champ **priorité**, attribuez une priorité à la règle.

Les règles sont validées par rapport à la demande de gestion entrante dans l'ordre croissant de leurs priorités. Si une règle correspond, l'action est exécutée et les règles suivantes en dessous de cette règle sont ignorées. Par exemple, si une adresse IP source 10.10.10.10 est configurée avec la priorité 1 pour autoriser, et que la même adresse IP source 10.10.10.10 est également configurée avec la priorité 2 pour refuser, l'accès est autorisé si le profil est actif et la deuxième règle est ignorée.

11. Cliquez sur le bouton **Add** (Ajouter).

La règle d'accès est ajoutée.

12. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Activez le profil d'accès.

Après avoir ajouté des règles au profil d'accès, vous pouvez activer le profil d'accès.

 **Attention:** Si vous configurez un profil d'accès de sécurité de manière incorrecte et que vous activez le profil d'accès, vous risquez de ne plus pouvoir accéder à l'interface utilisateur principale du commutateur. Si cette situation se produit, vous devez réinitialiser le commutateur aux paramètres par défaut (voir [Pour rétablir les paramètres par défaut du routeur](#) : à la page 1144).

Pour activer le profil d'accès :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > accès > contrôle d'accès > Configuration du profil d'accès**.

La page Configuration du profil d'accès s'affiche. La case désactiver le profil est cochée.

6. Cochez la case **Activer le profil**.

7. Cliquez sur le bouton **Apply** (Appliquer).

Vos paramètres sont enregistrés et le profil d'accès est maintenant actif.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Afficher le résumé du profil d'accès et le nombre de paquets filtrés

Après avoir ajouté des règles au profil actif, vous pouvez afficher les entrées dans le résumé. Si le profil d'accès est actif, vous pouvez également afficher le nombre de paquets filtrés.

Pour afficher le résumé du profil d'accès et le nombre de paquets filtrés :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > accès > contrôle d'accès > Configuration du profil d'accès**.

La page Configuration du profil d'accès s'affiche.

Le champ paquets filtrés affiche le nombre de paquets filtrés.

6. Pour actualiser la page avec les informations les plus récentes sur le commutateur, cliquez sur le bouton **Actualiser**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 169 : Résumé du profil de configuration du profil d'accès

Champ	Description
Type de règle	Action effectuée lorsque les règles correspondent.
Type de service	Type de service sélectionné. La stratégie est restreinte par le type de service sélectionné.
Adresse IP source	Adresse IP source du client à l'origine du trafic de gestion.
Masque	Masque de sous-réseau de l'adresse IP.
Priorité	Priorité de la règle.

Désactiver un profil d'accès .

Vous pouvez désactiver un profil d'accès.

Pour désactiver un profil d'accès :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > accès > contrôle d'accès > Configuration du profil d'accès** .

La page Configuration du profil d'accès s'affiche. La case Activer le profil est cochée.

6. Cochez la case **désactiver le profil**.

7. Cliquez sur le bouton **Apply** (Appliquer).

Vos paramètres sont enregistrés et le profil d'accès est maintenant désactivé.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimer un profil d'accès.

Vous pouvez supprimer une règle de trafic dont vous n'avez plus besoin. Avant de pouvoir supprimer le profil d'accès, vous devez désactiver informatique (voir [Désactiver un profil d'accès](#), à la page 898).

Pour supprimer un profil d'accès :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > accès > contrôle d'accès > Configuration du profil d'accès**.

La page Configuration du profil d'accès s'affiche. La case désactiver le profil est cochée.

6. Cochez la case **Supprimer le profil**.

7. Cliquez sur le bouton **Apply** (Appliquer).

Le profil d'accès est supprimé.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Authentification du port

Avec l'authentification basée sur le port, lorsque 802.1X est activé à la fois globalement et sur le port, l'authentification réussie de n'importe quel demandeur connecté au port permet à tous les utilisateurs d'utiliser le port sans restrictions. A tout moment, un seul demandeur est autorisé à tenter une authentification sur un port dans ce mode. Dans ce mode, les ports sont sous contrôle bidirectionnel. 802.1X est le mode d'authentification par défaut. 802.1X est également appelé dot1x.

❗ Remarque: Pour l'authentification de port, si nous faisons référence à un port, informatique signifie la même chose qu'une interface physique.

Un réseau 802.1X comprend trois composants :

- **Authentification.** Port authentifié avant que l'accès aux services système ne soit autorisé.
- **Demandeur :** Hôte connecté au port authentifié demandant l'accès aux services système.
- **Serveur d'authentification** Le serveur externe, par exemple, le serveur RADIUS qui effectue l'authentification au nom de l'authentificateur, et indique si le demandeur est autorisé à accéder aux services du système.

Configurez les paramètres d'authentification 802.1X globaux

Vous pouvez activer 802.1X sur le commutateur et configurer les paramètres 802.1X globaux qui s'appliquent au commutateur et à des utilisateurs spécifiques.

Si vous activez 802.1X, l'authentification doit être effectuée par un serveur RADIUS :

- **Serveur RADIUS.** Configurez un serveur RADIUS (voir [serveurs RADIUS](#) à la page 831).
- **Méthode d'authentification primaire :** Définissez la méthode d'authentification principale sur RADIUS, c'est-à-dire que RADIUS doit être la méthode 1 pour le paramètre defaultList de la liste d'authentification de connexion (voir [Configurez une liste d'authentification de connexion](#) à la page 850).

Pour configurer les paramètres 802.1X globaux :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > authentification du port > basique > Configuration 802.1X**.

La page Configuration 802.1X s'affiche.

6. Sélectionnez le bouton radio **désactiver** ou **Activer** le mode administrateur Dot1x :

- Sous tension L'authentification par port 802.1X est activée globalement sur le commutateur.
- Désactivé : L'authentification par port 802.1X est globalement désactivée sur le commutateur. Il s'agit de l'option par défaut. Le commutateur ne vérifie pas l'authentification 802.1X avant d'autoriser le trafic sur les ports, même si les ports individuels sont configurés pour autoriser uniquement les utilisateurs authentifiés.

7. Sélectionnez le bouton radio **désactiver** ou **Activer** le mode Admin d'authentification :

- Sous tension Le mode d'administration d'authentification est activé, ce qui nécessite que l'authentification soit effectuée par un serveur RADIUS. Cela signifie que la méthode d'authentification principale doit être RADIUS. Pour définir la méthode, sélectionnez sécurité > sécurité de gestion > liste d'authentification > liste d'authentification et sélectionnez **RADIUS** comme méthode 1 pour la liste

par défaut. Pour plus d'informations, consultez la section Configurez une liste d'authentification de connexion à la page 850.

- Désactivé : Le mode d'administration d'authentification est désactivé, ce qui correspond au paramètre par défaut. Le commutateur ne vérifie pas l'authentification 802.1X avant d'autoriser le trafic sur les ports, même si l'authentification basée sur les ports 802.1X est globalement activée (voir l'étape précédente) et que les ports sont configurés pour autoriser uniquement les utilisateurs authentifiés.
8. Sélectionnez le bouton radio **désactiver** ou **Activer** le mode d'affectation VLAN.
Lorsqu'elle est activée, cette fonctionnalité permet à un port d'être placé dans un VLAN particulier en fonction du résultat de l'authentification ou du type d'authentification 802.1X utilisé par un client lorsque informatique accède au périphérique. Le serveur d'authentification peut fournir des informations au dispositif sur le VLAN auquel attribuer le demandeur. La valeur par défaut est désactiver.
 9. Sélectionnez le bouton radio EAPOL Flood mode **Disable** ou **Enable**.
Cette sélection spécifie si la prise en charge du flood EAP (extensible Authentication Protocol) sur LAN (EAPOL) est activée sur le commutateur. La valeur par défaut est désactiver.
 10. Dans le menu **mode de création de VLAN dynamique**, sélectionnez **désactiver** ou **Activer**.
Si les VLAN attribués par RADIUS sont activés, le serveur RADIUS inclut l'ID VLAN dans les attributs de tunnel 802.1X de son message de réponse à l'unité. Si la création de VLAN dynamique est activée sur le terminal et que le VLAN attribué par RADIUS n'existe pas, le VLAN attribué est créé dynamiquement. Cela signifie que le client peut se connecter à partir de n'importe quel port et est affecté au VLAN approprié. Cette fonctionnalité permet aux clients de se déplacer sur le réseau sans nécessiter de configuration supplémentaire. La valeur par défaut est désactiver.
 11. Dans le menu **Monitor mode (mode moniteur)**, sélectionnez **Disable (désactiver)** ou **Enable(Activer)**.
Si elle est activée, cette option permet au commutateur de surveiller le processus d'authentification dot1x et peut vous aider à diagnostiquer les échecs d'authentification, le cas échéant. La valeur par défaut est désactiver.
 12. Dans le menu **utilisateurs**, sélectionnez le nom d'utilisateur auquel la liste de connexion que vous pouvez sélectionner à l'étape suivante doit s'appliquer.
 13. Dans le menu **connexion**, sélectionnez la liste de connexion qui s'applique au nom d'utilisateur que vous avez sélectionné à l'étape précédente.
Si 802.1X est activé, la liste dot1xList par défaut s'applique à l'authentification, comme indiqué dans le champ liste d'authentification.
Le champ version du logiciel affiche toujours 0.

14. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

15. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Gérer l'authentification de port sur des ports individuels .

Vous pouvez activer et configurer le contrôle d'accès aux ports sur un ou plusieurs ports physiques.

Configurer les paramètres 802.1X pour un port

Vous pouvez configurer les paramètres de contrôle d'accès au port 802.1X pour un ou plusieurs ports.

Pour configurer les paramètres 802.1X d'un port :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > authentification du port > Avancé > authentification du port**.

Port Authentication

1 All

☐	Port	Control Mode	Host Mode	MAB	MAB Auth Type	Outlet Period	Transmit Period	Guest VLAN ID	Unauthenticated VLAN ID	Max ReAuth Requests	Supplicant Timeout	Server Timeout	Maximum Requests	PAE Capabilities
☐	0/1	Auto	Multi-Domain-Multi-Host	Disable	N/A	60	30	0	0	2	30	30	2	Authenticator
☐	0/2	Auto	Multi-Domain-Multi-Host	Disable	N/A	60	30	0	0	2	30	30	2	Authenticator
☐	0/3	Auto	Multi-Domain-Multi-Host	Disable	N/A	60	30	0	0	2	30	30	2	Authenticator
☐	0/4	Auto	Multi-Domain-Multi-Host	Disable	N/A	60	30	0	0	2	30	30	2	Authenticator
☐	0/5	Auto	Multi-Domain-Multi-Host	Disable	N/A	60	30	0	0	2	30	30	2	Authenticator
☐	0/6	Auto	Multi-Domain-Multi-Host	Disable	N/A	60	30	0	0	2	30	30	2	Authenticator
☐	0/7	Auto	Multi-Domain-Multi-Host	Disable	N/A	60	30	0	0	2	30	30	2	Authenticator
☐	0/8	Auto	Multi-Domain-Multi-Host	Disable	N/A	60	30	0	0	2	30	30	2	Authenticator
☐	0/9	Auto	Multi-Domain-Multi-Host	Disable	N/A	60	30	0	0	2	30	30	2	Authenticator
☐	0/10	Auto	Multi-Domain-Multi-Host	Disable	N/A	60	30	0	0	2	30	30	2	Authenticator
☐	0/11	Auto	Multi-Domain-Multi-Host	Disable	N/A	60	30	0	0	2	30	30	2	Authenticator
☐	0/12	Auto	Multi-Domain-Multi-Host	Disable	N/A	60	30	0	0	2	30	30	2	Authenticator

La figure précédente montre une partie de la page uniquement.

6. Si une pile est configurée, indiquez si vous souhaitez afficher les interfaces physiques d'un commutateur ou de tous les commutateurs de la pile :

- **ID d'unité pour un commutateur empilé** : Les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
Si aucune pile de commutateurs n'est configurée, la seule option est l'ID d'unité 1.
- **Tous** : Les interfaces physiques de tous les commutateurs de la pile sont affichées.
Si aucune pile de commutateurs n'est configurée, l'option tous n'a aucun effet.

7. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :

- Pour afficher ou effacer les statistiques d'une seule interface, cochez la case associée à l'interface ou saisissez le numéro de l'interface dans le champ **aller à l'interface** et cliquez sur le bouton **aller**.
- Pour configurer plusieurs interfaces avec les mêmes paramètres, cochez la case associée à chaque interface.
- Pour configurer toutes les interfaces avec les mêmes paramètres, cochez la case dans la ligne d'en-tête.

8. Dans le menu **Control mode**, sélectionnez une option :

- **Auto**. L'entité d'accès au port d'authentification (PAE) définit le mode de port contrôlé pour refléter le résultat des échanges d'authentification entre le

demandeur, l'authentificateur et le serveur d'authentification. Il s'agit de l'option par défaut.

- **Autorisation forcée** L'authentificateur consultation définit sans condition le port contrôlé sur autorisé.
- **Forcer-non autorisé** L'authentificateur consultation définit sans condition le port contrôlé sur non autorisé.

9. Dans le menu **Host mode**, sélectionnez une option pour spécifier le nombre et le type de clients qui peuvent être authentifiés et autorisés sur le port :

- **Hôte unique** : Un seul client de données peut être authentifié sur le port. Une fois l'authentification réussie, l'accès est accordé à ce client uniquement, mais pas aux autres clients. Ce n'est que lorsque ce client se déconnecte qu'un autre client peut être authentifié et autorisé sur le port et autorisé à accéder au port.
- **Multi-hôte** : Initialement, un seul client de données peut être authentifié sur le port. Une fois l'authentification réussie, l'accès est accordé à tous les clients connectés au port.

Par exemple, utilisez cette option lorsqu'un point d'accès WiFi est connecté à un port à accès contrôlé d'un NAS. Une fois le point d'accès authentifié par le NAS, le port est autorisé pour le trafic provenant non seulement du point d'accès, mais également de tous les clients WiFi connectés au point d'accès.

- **Multi-domaine** : Un client de données et un client vocal peuvent être authentifiés sur le port. Une fois l'authentification réussie, les clients de données et voix se voient accorder l'accès.

Par exemple, utilisez cette option lorsqu'un téléphone IP est connecté à un port NAS et qu'un ordinateur portable est connecté au port Hub du téléphone IP. Les deux périphériques doivent être authentifiés pour accéder aux services réseau derrière le NAS. Les domaines voix et données sont séparés. (L'attribut de serveur RADIUS Cisco-AVPair = classe-traffic-périphérique=voix est utilisé pour identifier un client vocal.)

- **Multi-Auth** : Un client voix et plusieurs clients données peuvent être authentifiés sur le port. Une fois l'authentification réussie, l'accès est accordé à tous les clients.

Par exemple, utilisez cette option lorsqu'un réseau d'ordinateurs portables et un téléphone IP sont connectés à un port NAS via un concentrateur.

- **Multi-domaine-Multi-hôte** : Initialement, un client voix et un client données peuvent être authentifiés sur le port. Une fois le client de données authentifié, l'accès est accordé à tous les clients connectés au port et ils sont considérés comme des clients de données.

Par exemple, utilisez cette option lorsqu'un téléphone IP est connecté à un port NAS et qu'un contrôleur de machine virtuelle (VM) est connecté au port Hub du téléphone IP. Le contrôleur VM héberge plusieurs VM. Le contrôleur VM et le

téléphone IP doivent être authentifiés pour accéder aux services réseau derrière le NAS. Les domaines voix et données sont séparés. Une fois le contrôleur de VM authentifié, le trafic est autorisé à partir de toutes les VM hébergées par le contrôleur de VM. Notez que si le client de données est authentifié en premier, le client vocal ne peut être authentifié qu'à l'aide de la norme 802.1x.

10. Dans le menu **MAB**, sélectionnez pour activer ou désactiver le contournement de l'authentification MAC (MAB) pour les clients non conscients 802.1x.

MAB fonctionne uniquement si le mode de contrôle de port est basé sur MAC. La sélection par défaut est désactiver.

11. Dans le menu **MAB Auth type**, sélectionnez une option d'authentification MAB :

- EAP-MD5 : Le hachage MD5 de l'adresse MAC est envoyé comme mot de passe dans le message EAP (attribut Radius 79) au serveur d'authentification.
- PAP L'adresse MAC du client est envoyée comme mot de passe, similaire au format de l'attribut 1, en texte clair dans le message User-Password (attribut Radius 2).
- CHAP Une vérification de 16 octets générée aléatoirement est envoyée en tant que message de vérification CHAP (attribut Radius 60) avec le message de mot de passe CHAP (attribut Radius 3). L'ID CHAP est un numéro unique utilisé pour identifier la session. L'adresse MAC du client est récupérée et formatée à l'aide du format attribut 1 configuré. Ensuite, ces informations sont utilisées comme secret pour dériver les informations pour le message CHAP-Password. Les informations du message CHAP-Password sont calculées comme MD5 (avec l'ID CHAP, secret et défi CHAP).

12. Dans le champ **Quiet Period**, saisissez la période en secondes pendant laquelle l'interface ne tente pas d'acquiescer un demandeur après un échec d'un échange d'authentification antérieur.

Entrez une valeur comprise entre 0 et 65535. Une période de silence de 0 signifie que l'interface n'acquiesce aucun demandeur. La valeur par défaut est de 60 secondes.

13. Dans le champ **période de transmission**, entrez la période en secondes après laquelle l'interface envoie une trame requête EAP/identité EAPOL au demandeur.

Entrez une valeur comprise entre 0 et 65535. La valeur par défaut est de 30 secondes.

14. Dans le champ **GuestVLAN ID**, entrez l'ID du VLAN invité.

Entrez une valeur comprise entre 0 et 4093. Le numéro par défaut est 0.

15. Dans le champ **ID VLAN non authentifié**, entrez l'ID de l'ID VLAN non authentifié

Un utilisateur a le droit de saisir les informations d'identification correctes à trois reprises. Sinon, le client est placé dans le VLAN non authentifié. Entrez une valeur comprise entre 0 et 4093. Le numéro par défaut est 0.

16. Dans le champ **Max ReAuth Requests**, entrez le nombre maximal de demandes de réauthentification autorisées.
Entrez une valeur comprise entre 1 et 20. La valeur par défaut est 2.
17. Dans le champ **délai d'attente du demandeur**, entrez la période en secondes après laquelle l'interface expire le délai d'attente du demandeur.
Entrez une valeur comprise entre 0 et 65535. La valeur par défaut est de 30 secondes.
18. Dans le champ **délai du serveur**, entrez la période après laquelle l'interface expire le serveur d'authentification.
Entrez une valeur comprise entre 0 et 65535. La valeur par défaut est de 30 secondes.
19. Dans le champ **nombre maximal de demandes**, entrez le nombre maximal de fois que l'interface envoie une demande/identité EAP EAPOL au demandeur avant d'expirer le délai d'attente du demandeur.
Entrez une valeur comprise entre 1 et 10. Le numéro par défaut est 2.
20. Dans le menu **fonctionnalités de consultation**, sélectionnez **authentificateur** ou **demandeur** pour spécifier la fonction de l'entité d'accès au port (consultation).
La valeur par défaut est Authenticator.
21. Dans le menu **réauthentification périodique**, sélectionnez pour activer ou désactiver l'option de réauthentification périodique du demandeur.
La valeur par défaut est désactiver.
22. Si vous activez l'option de réauthentification périodique, dans le champ **période de réauthentification**, entrez la période en secondes après laquelle le demandeur doit être réauthentifié.
Entrez une valeur comprise entre 0 et 65535. La valeur par défaut est de 3600 secondes.
23. Dans le menu **privilèges d'utilisateur**, sélectionnez **admin** ou **guest** pour limiter le type d'utilisateurs auxquels l'accès peut être accordé.
Par défaut, les utilisateurs admin et invités peuvent se voir accorder l'accès.
24. Dans le champ **nombre maximal d'utilisateurs**, entrez le nombre maximal de demandeurs que l'interface peut prendre en charge.
Le numéro par défaut est 48.
25. Dans les colonnes ordre d'authentification, entrez l'ordre dans lequel l'authentification doit se produire pour trois méthodes maximum :

- Méthode 1 : La sélection par défaut est DOT1X. Les autres options sont MAB et PORTAIL CAPTIF. Vous ne pouvez pas désactiver la méthode 1.
- Méthode 2 : La sélection par défaut est MAB. Les autres options sont aucun, DOT1X et PORTAIL CAPTIF. Désactivez la méthode 2 en sélectionnant **aucun**.
- Méthode 3 : La sélection par défaut est PORTAIL CAPTIF. Les autres options sont aucun, DOT1X et MAB. Désactivez la méthode 3 en sélectionnant **aucun**.

Par exemple, si un client tente une authentification 802.1X (basée sur les informations d'identification de l'utilisateur et du client) et que l'authentification échoue, l'interface procède à l'authentification MAB. Si cette méthode échoue également, l'interface procède à l'authentification du portail captif. Si cette méthode échoue également, le client ne peut pas être authentifié.

26. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

27. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Initialisez 802.1X sur un port

Si vous initialisez 802.1X sur un port, le port devient non autorisé et passe ensuite par la procédure d'authentification, ce qui bloque le trafic sur le port jusqu'à ce que le port soit autorisé avec succès.

Vous ne pouvez initialiser 802.1X sur un port que si le mode de contrôle est défini sur Auto. Il s'agit du paramètre par défaut, dans lequel l'entité d'accès au port d'authentification (PAE) définit le mode de port contrôlé pour refléter le résultat des échanges d'authentification entre le demandeur, l'authentificateur et le serveur d'authentification.

Pour initialiser 802.1X sur un port :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > authentification du port > Avancé > authentification du port**.

La page authentification du port s'affiche.

6. Si une pile est configurée, indiquez si vous souhaitez afficher les interfaces physiques d'un commutateur ou de tous les commutateurs de la pile :

- **ID d'unité pour un commutateur empilé** : Les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
Si aucune pile de commutateurs n'est configurée, la seule option est l'ID d'unité 1.
- **Tous** : Les interfaces physiques de tous les commutateurs de la pile sont affichées.
Si aucune pile de commutateurs n'est configurée, l'option tous n'a aucun effet.

7. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :

- Pour afficher ou effacer les statistiques d'une seule interface, cochez la case associée à l'interface ou saisissez le numéro de l'interface dans le champ **aller à l'interface** et cliquez sur le bouton **aller**.
- Pour configurer plusieurs interfaces avec les mêmes paramètres, cochez la case associée à chaque interface.
- Pour configurer toutes les interfaces avec les mêmes paramètres, cochez la case dans la ligne d'en-tête.

8. Cliquez sur le bouton **initialiser**.

802.1X sur le port sélectionné est réinitialisé à l'état d'initialisation. Le trafic envoyé vers et depuis le port est bloqué pendant le processus d'authentification. Ce bouton n'est disponible que si le mode de commande est auto. Lorsque vous cliquez sur ce bouton, l'action est immédiate. Il n'est pas nécessaire de cliquer sur le bouton **appliquer** pour que l'action se produise.

Afficher le résumé des ports

Vous pouvez afficher des informations récapitulatives sur les paramètres d'authentification basés sur les ports pour chaque port.

Pour afficher le résumé des ports :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > authentification du port > Avancé > Résumé du port**.

La page Port Summary s'affiche.

6. Si une pile est configurée, indiquez si vous souhaitez afficher les interfaces physiques d'un commutateur ou de tous les commutateurs de la pile :

- **ID d'unité pour un commutateur empilé** : Les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.

Si aucune pile de commutateurs n'est configurée, la seule option est l'ID d'unité 1.

- **Tous** : Les interfaces physiques de tous les commutateurs de la pile sont affichées.

Si aucune pile de commutateurs n'est configurée, l'option tous n'a aucun effet.

7. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

Le tableau suivant décrit les champs en lecture seule de la page.

Table 170 : Informations récapitulatives sur le port

Champ	Description
Port	Port pour lequel les paramètres sont affichés
Mode de contrôle	Mode de contrôle configuré pour le port : • Forcer-non autorisé L'entité d'accès au port d'authentification (PAE) définit de manière inconditionnelle le port contrôlé sur non autorisé. • Autorisation forcée L'authentificateur consultation définit sans condition le port contrôlé sur autorisé. • Auto. L'authentificateur PAE définit le mode de port contrôlé pour refléter le résultat des échanges d'authentification entre le demandeur, l'authentificateur et le serveur d'authentification.
Mode de commande de fonctionnement	Mode de contrôle sous lequel le port fonctionne réellement. Les options sont les suivantes : • ForceUnauthorized • ForceAuthorized • Automatique • Basé sur MAC • N/A Si le port est à l'état détaché, la valeur est N/A car le port ne peut pas participer au contrôle d'accès au port.
Réauthentification activée	Indique si la réauthentification du demandeur est autorisée. Si la valeur est true, la réauthentification est autorisée. Sinon, la réauthentification n'est pas autorisée.
Sens de commande	La direction de contrôle, qui détermine le degré auquel les échanges de protocole se produisent entre un demandeur et un authentificateur. La direction détermine si le port contrôlé non autorisé exerce un contrôle sur la communication dans les deux sens (désactivant les trames entrantes et sortantes) ou juste dans le sens entrant (désactivant uniquement la réception des trames entrantes).
Fonctionnalités de consultation	Fonctionnalité d'entité d'accès au port (PAE), qui est authentificateur ou demandeur
État consultation de l'authentificateur	L'état de l'authentificateur consultation : • Initialisation • Authentification en cours... • Authentification • Maintenu • Non authentifié
Transmission clé activée	Indique si la transmission de clé est activée. Si la valeur est False, la transmission de clé n'a pas lieu. Sinon, la transmission de clé est prise en charge.

Table 170 : Informations récapitulatives sur le port (A continué)

Champ	Description
Etat du port	Statut d'autorisation du port : • N/A Si le port est à l'état détaché, la valeur est N/A car le port ne peut pas participer au contrôle d'accès au port. • Autorisé • Non autorisé
Version du protocole	La version du protocole est toujours 2, correspondant à la deuxième version de la spécification 802.1X.

Afficher le résumé du client

Vous pouvez afficher des informations sur les périphériques demandeurs connectés aux ports d'authentification locaux. S'il n'existe aucune session 802.1X active, la table est vide.

Pour afficher le résumé du client :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > authentification du port > Avancé > Récapitulatif du client**.

La page Client Summary s'affiche.

6. Si une pile est configurée, indiquez si vous souhaitez afficher les interfaces physiques d'un commutateur ou de tous les commutateurs de la pile :

- **ID d'unité pour un commutateur empilé** : Les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
Si aucune pile de commutateurs n'est configurée, la seule option est l'ID d'unité 1.
- **Tous** : Les interfaces physiques de tous les commutateurs de la pile sont affichées.
Si aucune pile de commutateurs n'est configurée, l'option tous n'a aucun effet.

7. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

Le tableau suivant décrit les champs en lecture seule de la page.

Table 171 : Informations récapitulatives sur le client

Champ	Description
Port	Interface pour laquelle les informations sont affichées.
Nom d'utilisateur	Nom représentant l'identité du périphérique demandeur
Adresse Mac du demandeur	Adresse MAC du périphérique du demandeur
Durée de la session	Période en secondes depuis que le demandeur s'est connecté
ID filtre	ID de filtre de stratégie attribué par l'authentificateur au terminal demandeur
Identifiant VLAN	ID VLAN attribué par l'authentificateur au périphérique demandeur
VLAN assigné	Motif de l'ID VLAN attribué par l'authentificateur au périphérique demandeur : • VLAN assigné par défaut : Le client a été authentifié sur le port VLAN par défaut et le serveur d'authentification n'était pas un serveur RADIUS • VLAN assigné RADIUS : RADIUS a été utilisé pour authentifier le client • VLAN non authentifié : Le client a été authentifié sur le VLAN non authentifié • VLAN invité Le client a été authentifié sur le VLAN invité • VLAN Voice Le client a été authentifié sur Voice VLAN • Mode moniteur VLAN : Le client a été authentifié en mode moniteur et affecté par le serveur RADIUS à un VLAN moniteur • Non attribué : Le client n'a été affecté à aucun VLAN
Expiration de la session	Expiration de session appliquée par le serveur RADIUS pour le périphérique demandeur

Table 171 : Informations récapitulatives sur le client (A continué)

Champ	Description
Action de résiliation	Action de résiliation appliquée par le serveur RADIUS pour le périphérique demandeur
Temps restant pour l'action de fin de session	Temps restant avant la fin de la session pour la raison affichée dans le champ action de fin

Filtres MAC pour le contrôle du trafic

Vous pouvez créer des filtres MAC qui limitent le trafic autorisé à entrer et sortir des ports spécifiés sur le commutateur. Les limitations de trafic sont basées sur les adresses MAC.

Créez un filtre MAC

Vous pouvez créer des filtres MAC qui limitent le trafic autorisé à entrer et sortir des ports spécifiés sur le système.

Pour créer un filtre MAC :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > contrôle du trafic > filtre MAC**.

MAC Filter Configuration

MAC Filter Create Filter ▾

VLAN ID

MAC Address

Source Port Members

Ports

Ports 1 3 5 7 9 11
2 4 6 8 10 12

LAG

LAG 1 3 5 7
2 4 6 8

Destination Port Members

Ports

Ports 1 3 5 7 9 11
2 4 6 8 10 12

LAG

LAG 1 3 5 7
2 4 6 8

6. Dans le menu **filtre MAC**, sélectionnez **créer un filtre**.

Si vous n'avez configuré aucun filtre, c'est la seule option disponible.

7. Dans le menu **VLAN ID**, sélectionnez l'VLAN à utiliser avec l'adresse MAC.

8. Dans le champ **adresse MAC**, spécifiez l'adresse MAC du filtre au format XX:XX:XX:XX:XX:XX.

Vous ne pouvez pas définir de filtres pour les adresses MAC suivantes :

- 00:00:00:00:00:00
- 01:80:C2:00:00:00 À 01:80:C2:00:00:0F
- 01:80:C2:00:00:20 à 01:80:C2:00:00:21
- FF:FF:FF:FF:FF:FF

9. Dans la table ports (ou, si une pile est configurée, dans les tables ports) et dans la table lag de la section Membres des ports source, sélectionnez les ports et LAG qui doivent être inclus dans le filtre entrant.

Les ports du commutateur (unité 1) sont affichés. Si une pile est configurée, les ports de chaque commutateur empilé (unité 1, unité 2, etc.) sont affichés et vous pouvez sélectionner des ports sur différents commutateurs empilés.

Si un paquet avec l'adresse MAC et l'ID VLAN que vous spécifiez est reçu sur un port ou un lag qui ne fait pas partie du filtre entrant, le paquet est abandonné.

10. Dans la table ports (ou, si une pile est configurée, dans les tables ports) et dans la table et lag de la section Membres du port de destination, sélectionnez les ports et LAG à inclure dans le filtre sortant.

Dans cette section, les ports du commutateur (unité 1) sont également affichés. Si une pile est configurée, les ports de chaque commutateur empilé (unité 1, unité 2, etc.) sont affichés et vous pouvez sélectionner des ports sur différents commutateurs empilés.

Un paquet avec l'adresse MAC et l'ID VLAN que vous spécifiez ne peut être transmis qu'à partir d'un port ou d'un lag faisant partie du filtre sortant.

❗ Remarque: Les ports de destination ne peuvent être inclus que dans un filtre multicast. Un filtre multicast est déterminé par l'adresse MAC que vous entrez dans le champ adresse MAC.

11. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

12. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimer un filtre MAC

Vous pouvez supprimer un filtre MAC existant dont vous n'avez plus besoin.

Pour supprimer un filtre MAC :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.
4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **sécurité > contrôle du trafic > filtre MAC** .
La page Configuration du filtre MAC s'affiche.
6. Dans le menu **filtre MAC**, sélectionnez le filtre MAC.
7. Cliquez sur le bouton **Supprimer**.
Le filtre est retiré.
8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Affichez le résumé du filtre MAC

Vous pouvez afficher les filtres MAC configurés sur le commutateur.

Pour afficher le résumé du filtre MAC :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > contrôle du trafic > filtre MAC > Résumé du filtre MAC**

La page Résumé du filtre MAC s'affiche.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 172 : Informations récapitulatives du filtre MAC

Champ	Description
Adresse MAC	Adresse MAC du filtre au format XX :XX :XX :XX :XX :XX.
Identifiant VLAN	ID VLAN utilisé avec l'adresse MAC pour identifier entièrement les paquets que vous souhaitez filtrer.
Membres du port source	Ports à utiliser pour filtrer les paquets entrants.
Membres du port de destination	Ports à utiliser pour filtrer les paquets sortants.

Sécurité portuaire

La sécurité des ports vous permet de verrouiller un ou plusieurs ports sur le commutateur. Lorsqu'un port est verrouillé, le port ne peut transférer des paquets que si le nombre total d'adresses MAC apprises dynamiquement et le nombre total d'adresses MAC ajoutées statiquement ne sont pas dépassés. Vous pouvez définir les seuils pour ces nombres. Une fois un seuil dépassé, le port rejette tous les autres paquets.

Vous pouvez également convertir des adresses MAC apprises dynamiquement en adresses MAC statiques et autoriser le trafic à partir de ces adresses MAC sur un port.

Configurez le mode de sécurité du port global

Avant de pouvoir activer et configurer la sécurité des ports individuels, vous devez activer globalement le mode de sécurité des ports pour le commutateur.

Pour configurer le mode de sécurité du port global :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > contrôle du trafic > sécurité des ports > Administration des ports**.

La page Administration des ports s'affiche.

6. Pour activer la sécurité du port sur le commutateur, sélectionnez le bouton radio **Activer** le mode de sécurité du port.

La valeur par défaut est désactiver.

7. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

Le tableau violations de la sécurité des ports affiche des informations sur les violations qui se sont produites sur les ports dont la sécurité est activée.

Table 173 : Informations sur les violations de sécurité portuaire

Champ	Description
Port	Port pour lequel la violation est affichée.
Dernière violation MAC	Adresse MAC source du dernier paquet rejeté sur le port verrouillé.
Identifiant VLAN	ID VLAN correspondant à la dernière violation d'adresse MAC.

Configurer une interface de sécurité de port

Une adresse MAC peut être définie comme autorisée par l'une des deux méthodes suivantes : dynamiquement ou statiquement. Les deux méthodes sont utilisées simultanément lorsqu'un port est verrouillé.

Le verrouillage dynamique met en oeuvre un premier mécanisme d'arrivée pour la sécurité portuaire. Vous spécifiez le nombre d'adresses pouvant être apprises sur le port verrouillé. Si la limite n'est pas atteinte, un paquet avec une adresse MAC source inconnue est appris et transmis normalement. Si la limite est atteinte, plus aucune adresse n'est apprise sur le port. Tous les paquets avec des adresses MAC source qui ne sont pas déjà apprises sont rejetés. Vous pouvez désactiver efficacement le verrouillage dynamique en définissant le nombre d'entrées dynamiques autorisées sur zéro.

Le verrouillage statique vous permet de spécifier une liste d'adresses MAC autorisées sur un port. Le comportement des paquets est le même que pour le verrouillage dynamique : seuls les paquets avec une adresse MAC source autorisée peuvent être transmis.

Pour configurer les paramètres de sécurité des ports :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > contrôle du trafic > sécurité des ports > Configuration de l'interface**.

La page Configuration de l'interface s'affiche.

6. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :

- **1 ou ID d'unité pour un commutateur empilé :**

- 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
 - **ID d'unité pour un commutateur empilé** : Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
 - LAG Seuls les LAG sont affichés.
 - **Tous**: Les interfaces physiques et les LAG sont affichés, ou pour une pile de commutateurs, les interfaces physiques de tous les commutateurs de la pile et les LAG sont affichés.
7. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :
- Pour afficher ou effacer les statistiques d'une seule interface, cochez la case associée à l'interface ou saisissez le numéro de l'interface dans le champ **aller à l'interface** et cliquez sur le bouton **aller**.
 - Pour configurer plusieurs interfaces avec les mêmes paramètres, cochez la case associée à chaque interface.
 - Pour configurer toutes les interfaces avec les mêmes paramètres, cochez la case dans la ligne d'en-tête.
8. Spécifiez les paramètres suivants :
- Mode de sécurité Activer ou désactiver la fonction de sécurité du port. La valeur par défaut est désactiver.
 - **Adresse MAC max apprise** : Spécifiez le nombre maximal d'adresses MAC apprises dynamiquement. La valeur par défaut est 4096. Si vous spécifiez 0, l'interface n'apprend aucune adresse MAC.
 - **Adresse MAC statique max** : Spécifiez le nombre maximal d'adresses MAC verrouillées statiquement. La valeur par défaut est 48.
 - **Arrêt pour violation** : Activer ou désactiver l'arrêt si un paquet avec une adresse MAC non autorisée est reçu. La valeur par défaut est désactiver.
 - **Interruption de violation** : Activer ou désactiver l'envoi d'interruptions de violation si un paquet avec une adresse MAC non autorisée est reçu. La valeur par défaut est désactiver.
9. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Afficher les adresses MAC apprises et les convertir en adresses statiques

Après avoir activé la sécurité des ports globalement (voir [Configurez le mode de sécurité du port global](#) à la page 919) et activé la sécurité des ports pour des interfaces spécifiques (voir [Configurer une interface de sécurité de port](#) à la page 920), vous pouvez convertir une adresse MAC apprise dynamiquement en une adresse verrouillée statiquement.

Pour afficher les adresses MAC apprises pour une interface individuelle ou un lag et convertir ces adresses MAC en adresses MAC statiques :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > contrôle du trafic > sécurité des ports > adresse MAC dynamique**.

La page adresse MAC dynamique s'affiche.

6. Pour afficher les adresses MAC apprises pour une interface, dans le menu **liste des ports**, sélectionnez l'interface ou le lag.

Le champ nombre d'adresses MAC dynamiques apprises affiche le nombre d'adresses MAC apprises dynamiquement sur un port spécifique.

Le tableau suivant présente les adresses MAC et leurs VLAN associés appris sur l'interface sélectionnée.

Champ	Description
Identifiant VLAN	ID VLAN correspondant à l'adresse MAC.
Adresse MAC	Adresses MAC apprises sur le port.

7. Pour convertir les adresses MAC apprises dynamiquement sur l'interface en adresses verrouillées statiquement, cochez la case **convertir l'adresse dynamique en adresse statique**.

Les entrées d'adresses MAC dynamiques sont converties en entrées d'adresses MAC statiques dans un ordre numérique croissant jusqu'à ce que la limite statique soit atteinte.

8. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

9. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Ajoutez une adresse MAC statique à la table d'adresses MAC pour la sécurité des ports

Les entrées d'adresses MAC statiques sont celles que vous ajoutez manuellement à la table d'adresses MAC pour la sécurité des ports d'une interface et d'un VLAN spécifiques.

Pour ajouter une adresse MAC statique à la table d'adresses MAC pour la sécurité du port :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.
4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **sécurité > contrôle du trafic > sécurité des ports > adresse MAC statique** .
La page adresse MAC statique s'affiche.
6. Dans le menu **interface**, sélectionnez l'interface ou lag.
7. Dans le champ **adresse MAC statique**, entrez l'adresse MAC.
8. Dans le menu **VLAN ID**, sélectionnez l'ID VLAN qui doit être associé à l'adresse MAC.
9. Cliquez sur le bouton **Add** (Ajouter).
L'adresse MAC statique est ajoutée à la table des adresses MAC.
10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimez une adresse MAC statique de la table d'adresses MAC pour la sécurité du port

Vous pouvez supprimer une adresse MAC statique dont vous n'avez plus besoin pour la sécurité du port.

Pour supprimer une adresse MAC statique de la table d'adresses MAC pour la sécurité du port :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > contrôle du trafic > sécurité des ports > adresse MAC statique**.

La page adresse MAC statique s'affiche.

6. Dans le menu **interface**, sélectionnez l'interface ou lag.

7. Cochez la case correspondant à l'adresse MAC.

8. Cliquez sur le bouton **Supprimer**.

L'adresse MAC statique est supprimée de la table d'adresses MAC.

9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Groupe de ports privés

Pour ajouter un niveau de sécurité, vous pouvez configurer un groupe privé de ports physiques (pas de LAG) qui peut fonctionner en mode isolé ou en mode communauté :

- **Groupe de mode isolé** : Un port que vous ajoutez en tant que membre du groupe ne peut pas transférer son trafic de sortie aux autres membres du même groupe.
- **Groupe de mode communautaire** : Un port que vous ajoutez en tant que membre du groupe *peut* transférer son trafic de sortie aux autres membres du même groupe, mais pas aux membres des autres groupes.

Ajoutez un groupe de ports privés

Après avoir ajouté un groupe privé, vous pouvez ajouter des membres au groupe (voir [Configurer l'appartenance à un groupe de ports privés](#) à la page 929).

Pour ajouter un groupe de ports privés :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > contrôle du trafic > Groupe privé > Configuration du groupe privé**.

La page Configuration de groupe privé s'affiche.

6. Dans le champ **nom du groupe**, entrez le nom du groupe privé.

Le nom peut comporter jusqu'à 24 caractères.

7. Dans le menu **Group mode**, sélectionnez le mode du groupe privé :

- **Isolé** : Un port que vous ajoutez en tant que membre du groupe ne peut pas transférer son trafic de sortie aux autres membres du même groupe.
- **Communauté** : Un port que vous ajoutez en tant que membre du groupe *peut* transférer son trafic de sortie aux autres membres du même groupe, mais pas aux membres des autres groupes.

8. Cliquez sur le bouton **Add** (Ajouter).

Le groupe privé est ajouté.

9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimer un groupe de ports privés

Vous pouvez supprimer un groupe de ports privés dont vous n'avez plus besoin.

Pour supprimer un groupe de ports privés :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > contrôle du trafic > Groupe privé > Configuration du groupe privé**.

La page Configuration de groupe privé s'affiche.

6. Cochez la case en regard du groupe privé.

7. Cliquez sur le bouton **Supprimer**.

Le groupe privé est supprimé.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurer l'appartenance à un groupe de ports privés

Après avoir ajouté un groupe de ports privés, vous pouvez ajouter des membres au groupe (voir [Ajoutez un groupe de ports privés](#) à la page 927).

Pour configurer l'appartenance à un groupe de ports privés :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > contrôle du trafic > Groupe privé > appartenance à un groupe privé**.

La page appartenance à un groupe privé s'affiche.

6. Dans le menu **ID de groupe**, sélectionnez l'ID de groupe.

7. Dans la table ports (ou, si une pile est configurée, dans l'une des tables ports), sélectionnez les ports qui doivent être membres du groupe.

Les ports du commutateur (unité 1) sont affichés. Si une pile est configurée, les ports de chaque commutateur empilé (unité 1, unité 2, etc.) sont affichés et vous pouvez sélectionner des ports sur différents commutateurs empilés.

8. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 174 : Informations sur l'appartenance à un groupe privé

Champ	Description
Nom du groupe	Nom du groupe privé
Mode Groupe	Le mode du groupe privé (communautaire ou isolé)

Protection des ports

Si un port est configuré comme protégé, informatique ne transfère le trafic vers aucun autre port protégé du commutateur, mais informatique le transfère vers des ports non protégés. Vous pouvez configurer les ports comme protégés ou non protégés.

Pour configurer des ports protégés :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > contrôle du trafic > ports protégés**.

La page ports protégés s'affiche.

6. Dans la liste **ID de groupe**, sélectionnez **0**, **1** ou **2** pour combiner les ports protégés sélectionnés dans un groupe logique.

Le trafic peut circuler entre des ports protégés appartenant à des groupes différents, mais pas au sein du même groupe. L'ID de groupe peut être 0, 1 ou 2.

7. Pour associer un nom au groupe de ports protégés, spécifiez un nom dans le champ **nom du groupe**.

Le nom peut comporter jusqu'à 32 caractères alphanumériques, espaces compris.

8. Dans la table ports (ou, si une pile est configurée, dans l'une des tables ports), sélectionnez les ports qui doivent être des ports protégés et les membres du groupe de ports protégés.

Les ports du commutateur (unité 1) sont affichés. Si une pile est configurée, les ports de chaque commutateur empilé (unité 1, unité 2, etc.) sont affichés et vous pouvez sélectionner des ports sur différents commutateurs empilés.

Par défaut, tous les ports ne sont pas protégés.

9. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

VLAN privés

Un VLAN privé contient des ports de commutateur qui ne peuvent pas communiquer entre eux, mais peuvent accéder à un autre réseau. Ces ports sont appelés ports privés. Chaque VLAN privé contient un ou plusieurs ports privés et un seul port de liaison montante ou groupe d'agrégation de liaison montante. Notez que tout le trafic entre les ports privés est bloqué sur toutes les couches, pas seulement le trafic de couche 2, mais aussi le trafic FTP, HTTP et Telnet.

Un VLAN privé sépare un domaine VLAN normal en deux sous-domaines ou plus. Chaque sous-domaine est défini (représenté) par un VLAN primaire et un VLAN secondaire :

- **VLAN primaire** : L'ID VLAN principal est le même pour tous les sous-domaines appartenant à un VLAN privé.
- **VLAN secondaire** : L'ID VLAN secondaire différencie les sous-domaines les uns des autres et fournit une isolation de couche 2 entre les ports du même VLAN privé.

Dans un VLAN privé, trois types de VLAN peuvent exister :

- **VLAN primaire** : Le VLAN achemine le trafic des ports à promiscuité vers des ports isolés, des ports communautaires et d'autres ports à promiscuité dans le même

VLAN privé. Dans un VLAN privé, vous ne pouvez configurer qu'un seul VLAN principal. Tous les ports d'un VLAN privé partagent le même VLAN principal.

- **VLAN isolé** : Le VLAN est un VLAN secondaire qui transporte le trafic des ports isolés vers les ports promiscues. Dans un VLAN privé, vous pouvez configurer un seul VLAN isolé.
- **Communauté VLAN** : Le VLAN est un VLAN secondaire qui transfère le trafic entre les ports appartenant à la même communauté et vers les ports promiscues. Dans un VLAN privé, vous pouvez configurer plusieurs VLAN de communauté.

Dans un VLAN privé, le commutateur prend en charge quatre types de désignations de port spéciales :

- **Port hôte** : Le port est un port hôte membre d'un VLAN communautaire ou d'un VLAN isolé, qui sont tous deux des VLAN secondaires au sein du VLAN privé. Il existe deux sous-types de port hôte :
 - **Port communautaire** : Le port est membre d'une communauté VLAN. Un port communautaire peut communiquer avec d'autres ports communautaires et des ports promiscues.
 - **Port isolé** : Le port est membre d'un VLAN isolé. Un port isolé peut communiquer avec des ports de promiscuité.
- **Port promiscuité** : Le port est membre d'un VLAN primaire (au sein du Private VLAN) et peut communiquer avec tous les types de ports du Private VLAN, y compris d'autres ports promiscues, des ports communautaires et des ports isolés.
- **Port tronc promiscueux** : Le port est à la fois un port agrégé de liaison montante (par exemple, informatique peut connecter un routeur) et un port promiscuité qui peut être membre de plusieurs VLAN primaires (dans le VLAN privé) ainsi que de VLAN normaux. Le port traite le trafic balisé pour communiquer avec tous les types de ports dans les VLAN privés (y compris les ports à promiscuité, les ports communautaires et les ports isolés) et avec les ports dans les VLAN normaux.
- **Port de jonction isolé** : Le port est à la fois un port agrégé de liaison descendante (par exemple, informatique peut se connecter à plusieurs périphériques en aval) et peut être membre de plusieurs VLAN isolés (VLAN secondaires au sein de VLAN privés) ainsi que de VLAN normaux. Le port traite le trafic balisé pour communiquer avec les ports des VLAN isolés et avec les ports des VLAN normaux. Les périphériques en aval connectés au port agrégé isolé n'ont pas besoin de prendre en charge les VLAN privés.

Présentation des tâches de configuration Private VLAN

Pour configurer un VLAN privé permettant la communication entre les commutateurs d'un réseau, effectuez les tâches décrites dans les sections suivantes :

1. Attribuez un type de VLAN privé à un VLAN à la page 935.

Par défaut, un VLAN est un VLAN normal, vous devez donc affecter un type de VLAN privé à un VLAN.

2. Configurez une association VLAN privée avec un VLAN principal et secondaire à la page 936.

Un VLAN privé doit se composer d'un VLAN primaire unique et d'un ou plusieurs VLAN secondaires.

3. Configurez le mode de port VLAN privé à la page 939.

Un port doit être dans le mode de port correct pour participer à un VLAN privé. Par exemple, pour faire d'un port un membre d'une VLAN VLAN isolée ou communautaire, vous devez d'abord configurer le port en tant que port hôte.

4. Interface hôte VLAN privée : Attribuez l'interface aux VLAN principaux et secondaires à la page 942.

Pour un port que vous avez configuré pour fonctionner en mode hôte, configurez un VLAN principal unique et un VLAN secondaire unique.

5. Interface promiscuous Private VLAN : Attribuez l'interface aux VLAN principaux et secondaires à la page 946.

Pour un port que vous avez configuré pour fonctionner en mode promiscuité, configurez un VLAN principal unique et un ou plusieurs VLAN secondaires.

6. Interface de ligne de réseau promiscuous Private VLAN : Ajoutez des VLAN principaux et secondaires à la jonction à la page 950.

Pour un port que vous avez configuré pour fonctionner en mode *agrégation* promiscuité, ajoutez des VLAN primaires et secondaires à l'agrégation.

7. Interface de jonction isolée Private VLAN : Ajoutez des VLAN principaux et secondaires à la jonction à la page 953

Pour un port que vous avez configuré pour fonctionner en mode *jonction* isolée, ajoutez des VLAN principal et secondaire à la jonction.

8. Configurez les VLAN natifs et autorisés sur une interface de jonction VLAN privée à la page 956

Pour le port que vous avez configuré pour fonctionner en mode *agrégation* VLAN privée (en mode agrégation de proximité ou en mode agrégation isolée), configurez les VLAN natifs pour le trafic non balisé et les VLAN privés autorisés.

Attribuez un type de VLAN privé à un VLAN

À chaque VLAN, vous pouvez affecter un type de VLAN privé, qui peut être principal, isolé ou Communauté. Par défaut, un VLAN est un VLAN normal et reçoit le type VLAN privé non configuré.

Pour affecter un type de VLAN privé à un VLAN :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > contrôle du trafic > VLAN privé > Configuration du type de VLAN privé**.

La page Configuration du type de VLAN privé s'affiche.

6. Cochez les cases correspondant au contenu.

7. Dans le menu **Private VLAN type**, sélectionnez le type de Private VLAN :

- **Non configuré** : Le VLAN n'est pas un VLAN privé mais un VLAN régulier. Il s'agit de l'option par défaut.
 - **Principal** Le VLAN est un VLAN primaire qui transfère le trafic des ports à promiscuité vers des ports isolés, des ports communautaires et d'autres ports à promiscuité dans le même VLAN privé. Dans un VLAN privé, vous ne pouvez configurer qu'un seul VLAN principal. Tous les ports d'un VLAN privé partagent le même VLAN principal.
 - **Isolé** : Le VLAN est un VLAN secondaire qui transporte le trafic des ports isolés vers les ports promiscues. Dans un VLAN privé, vous pouvez configurer un seul VLAN isolé.
 - **Communauté** : Le VLAN est un VLAN secondaire qui transfère le trafic entre les ports appartenant à la même communauté et vers les ports promiscues. Dans un VLAN privé, vous pouvez configurer plusieurs VLAN de communauté.
8. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez une association VLAN privée avec un VLAN principal et secondaire

Vous pouvez configurer un VLAN privé en associant un VLAN principal unique à un ou plusieurs VLAN secondaires.

Pour configurer une association VLAN privée avec un VLAN principal et secondaire :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > contrôle du trafic > Private VLAN > Configuration de l'association Private VLAN**.

La page Configuration de l'association Private VLAN s'affiche.

6. Si vous modifiez une association Private VLAN existante, cochez la case correspondant à l'association Private VLAN.

7. Dans le menu **Primary VLAN**, sélectionnez l'ID VLAN principal du Private VLAN.

Cette sélection spécifie le VLAN principal dans le VLAN privé. Vous pouvez associer des VLAN secondaires dans le VLAN privé à ce VLAN principal.

Pour plus d'informations sur la configuration d'un VLAN principal pour le Private VLAN, reportez-vous à la section [Attribuez un type de VLAN privé à un VLAN](#) à la page 935.

8. Dans le champ **VLAN secondaires**, spécifiez un ou plusieurs VLAN secondaires pour le VLAN privé.

Cette sélection spécifie les VLAN secondaires (VLAN isolés, VLAN de communauté ou une combinaison des deux) dans le VLAN privé. Les VLAN secondaires sont associés au VLAN primaire dans le VLAN privé.

Vous pouvez spécifier un seul ID VLAN, une plage d'ID VLAN ou une combinaison des deux dans l'ordre, séparés par une virgule (,) :

- Vous pouvez spécifier un ID VLAN individuel, tel que 10.
- Vous pouvez spécifier les valeurs de plage VLAN séparées par un tiret, par exemple, 10-13.
- Vous pouvez spécifier la combinaison des deux séparés par des virgules, par exemple : 12,154043,100010052000

Pour plus d'informations sur la configuration d'un VLAN isolé ou communautaire pour le VLAN privé, reportez-vous à [Attribuez un type de VLAN privé à un VLAN](#) à la page 935 la section .

9. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 175 : Association Private VLAN

Champ	Description
VLAN isolé	Le VLAN isolé unique associé au VLAN primaire sélectionné.
Communauté VLAN(s)	Liste des VLAN de communauté associés au VLAN principal sélectionné.

Supprimer une association VLAN privée existante

Vous pouvez supprimer une association VLAN privée dont vous n'avez plus besoin.

Pour supprimer une association VLAN privée :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > contrôle du trafic > Private VLAN > Configuration de l'association Private VLAN**.

La page Configuration de l'association Private VLAN s'affiche.

6. Cochez la case de l'association Private VLAN.

7. Cliquez sur le bouton **Supprimer**.

Les paramètres sont enregistrés. L'association Private VLAN est supprimée.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez le mode de port VLAN privé

Un port doit être dans le mode de port correct pour participer à un VLAN privé.

Le mode de port de plan privé détermine si un port (ou lag) peut fonctionner en mode hôte pour un VLAN principal ou secondaire (dans un VLAN privé) ou en mode Promiscuous pour un VLAN promiscuous (dans un VLAN privé).

Vous pouvez également configurer un port (ou lag) pour qu'il fonctionne comme une jonction à promiscuité pour une liaison montante vers un routeur ou comme une jonction isolée pour une liaison descendante vers plusieurs périphériques. Ces types de ports de jonction VLAN privés peuvent transporter plusieurs VLAN privés ainsi que des VLAN normaux.

Pour configurer le mode de port VLAN privé :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > contrôle du trafic > VLAN privé > Configuration du mode de port VLAN privé**.

La page Configuration du mode de port VLAN privé s'affiche.

6. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :

- **1 ou ID d'unité pour un commutateur empilé :**
 - 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
 - **ID d'unité pour un commutateur empilé :** Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
- **LAG** Seuls les LAG sont affichés.
- **Tous:** Les interfaces physiques et les LAG sont affichés, ou pour une pile de commutateurs, les interfaces physiques de tous les commutateurs de la pile et les LAG sont affichés.

7. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :

- Pour afficher ou effacer les statistiques d'une seule interface, cochez la case associée à l'interface ou saisissez le numéro de l'interface dans le champ **aller à l'interface** et cliquez sur le bouton **aller**.
- Pour configurer plusieurs interfaces avec les mêmes paramètres, cochez la case associée à chaque interface.

8. Dans le menu **Port VLAN mode**, sélectionnez le mode de port Private VLAN :

- Général : Le port fonctionne en mode général et non en tant que port dans un VLAN privé. Il s'agit de l'option par défaut.
- Hôte : Le port fonctionne en mode hôte dans un VLAN privé. Dans ce mode, le port peut être membre d'une communauté VLAN ou VLAN isolée :
 - **Communauté VLAN** : Le port est membre d'un VLAN secondaire (au sein du Private VLAN) et peut communiquer avec d'autres ports communautaires et ports promiscues.
 - **VLAN isolé** : Le port est membre d'un VLAN secondaire (au sein du Private VLAN) et ne peut communiquer qu'avec les ports promiscuous.

Pour configurer un port hôte en tant que membre de VLAN spécifiques, reportez-vous à la section Interface hôte VLAN privée : Attribuez l'interface aux VLAN principaux et secondaires à la page 942.

- **Promiscuité** : Le port fonctionne en mode promiscuous dans un VLAN privé. Dans ce mode, le port peut communiquer avec tous les types de ports dans le VLAN privé, y compris les autres ports promiscues, les ports communautaires et les ports isolés.

Pour configurer un port promiscuité en tant que membre de VLAN spécifiques, reportez-vous à la section Interface promiscuous Private VLAN : Attribuez l'interface aux VLAN principaux et secondaires à la page 946.

- **Port tronc promiscueux** : Le port fonctionne en mode de jonction promiscuité à la fois comme port de jonction de liaison montante (par exemple, informatique peut connecter un routeur) et comme port promiscuité pouvant être membre de plusieurs VLAN primaires (dans le VLAN privé) ainsi que de VLAN normaux. Dans ce mode, le port traite le trafic balisé pour communiquer avec tous les types de ports dans les VLAN privés (y compris les ports promiscues, les ports communautaires et les ports isolés) et avec les ports dans les VLAN normaux.

Pour attribuer un port agrégé de promiscuité à des VLAN spécifiques, reportez-vous à la section Interface de ligne de réseau promiscuous Private VLAN : Ajoutez des VLAN principaux et secondaires à la jonction à la page 950.

- **Port de jonction isolé** : Le port fonctionne en mode agrégation isolée (par exemple, informatique peut se connecter à plusieurs périphériques en aval) et peut être membre de plusieurs VLAN isolés (VLAN secondaires au sein de VLAN privés) ainsi que de VLAN normaux. Dans ce mode, le port traite le trafic balisé

pour communiquer avec les ports des VLAN isolés et avec les ports des VLAN normaux. Les périphériques en aval connectés au port agrégé isolé n'ont pas besoin de prendre en charge les VLAN privés.

Pour attribuer un port agrégé isolé à des VLAN spécifiques, reportez-vous à la section Interface de jonction isolée Private VLAN : Ajoutez des VLAN principaux et secondaires à la jonction à la page 953.

9. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Interface hôte VLAN privée : Attribuez l'interface aux VLAN principaux et secondaires

Si vous configurez le mode de port VLAN privé d'une interface en tant qu'hôte (voir Configurez le mode de port VLAN privé à la page 939), vous pouvez affecter l'interface à un seul VLAN primaire et à un seul VLAN secondaire.

Pour attribuer une interface hôte VLAN privée à un VLAN principal et secondaire :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > contrôle du trafic > Private VLAN > Configuration de l'interface hôte Private VLAN**.

La page Configuration de l'interface hôte Private VLAN s'affiche.

6. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :

- **1 ou ID d'unité pour un commutateur empilé :**
 - 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
 - **ID d'unité pour un commutateur empilé :** Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
- **LAG** Seuls les LAG sont affichés.
- **Tous:** Les interfaces physiques et les LAG sont affichés, ou pour une pile de commutateurs, les interfaces physiques de tous les commutateurs de la pile et les LAG sont affichés.

7. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :

- Pour afficher ou effacer les statistiques d'une seule interface, cochez la case associée à l'interface ou saisissez le numéro de l'interface dans le champ **aller à l'interface** et cliquez sur le bouton **aller**.
- Pour configurer plusieurs interfaces avec les mêmes paramètres, cochez la case associée à chaque interface.

8. Dans le champ **VLAN principal de l'hôte**, spécifiez un ID VLAN principal.

Vous pouvez sélectionner un VLAN pour lequel vous avez configuré le type principal (voir [Attribuez un type de VLAN privé à un VLAN](#) à la page 935).

9. Dans le champ **VLAN secondaire de l'hôte**, spécifiez un ID VLAN secondaire.

Vous pouvez sélectionner un VLAN pour lequel vous avez configuré le type isolé ou Communauté, qui sont tous deux des types de VLAN secondaires au sein d'un VLAN privé (voir [Attribuez un type de VLAN privé à un VLAN](#) à la page 935).

10. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

Les champs Operational(s) (VLAN(s) opérationnel(s)) affichent les VLAN principal et secondaire qui fonctionnent sur l'interface hôte.

11. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Interface hôte VLAN privée : Supprimez l'interface des VLAN principal et secondaire

Vous pouvez supprimer une interface hôte VLAN privée des VLAN principaux et secondaires.

Pour supprimer une interface hôte VLAN privée des VLAN principal et secondaire :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > contrôle du trafic > Private VLAN > Configuration de l'interface hôte Private VLAN**.

La page Configuration de l'interface hôte Private VLAN s'affiche.

6. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :

- **1 ou ID d'unité pour un commutateur empilé :**

- 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
- **ID d'unité pour un commutateur empilé :** Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.

- LAG Seuls les LAG sont affichés.

- **Tous:** Les interfaces physiques et les LAG sont affichés, ou pour une pile de commutateurs, les interfaces physiques de tous les commutateurs de la pile et les LAG sont affichés.

7. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :

- **Pour configurer une interface unique, cochez la case associée au port ou tapez le numéro de port (par exemple g1) dans le champ aller à l'interface et cliquez sur le bouton aller.**
- Pour configurer plusieurs interfaces avec les mêmes paramètres, cochez la case associée à chaque interface.

L'interface que vous sélectionnez doit être configurée en mode hôte (voir [Configurez le mode de port VLAN privé](#) à la page 939).

8. Cliquez sur le bouton **Supprimer**.

Les paramètres sont enregistrés. L'interface est supprimée des VLAN primaire et secondaire.

9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Interface promiscuous Private VLAN : Attribuez l'interface aux VLAN principaux et secondaires

Si vous configurez le mode de port VLAN privé d'une interface sur Promiscuous (voir [Configurez le mode de port VLAN privé](#) à la page 939), vous pouvez affecter l'interface à un VLAN principal unique et à un ou plusieurs VLAN secondaires.

Pour attribuer une interface promiscuous VLAN privée à un VLAN principal et à des VLAN secondaires :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > contrôle du trafic > Private VLAN > Private VLAN Promiscuous interface Configuration**.

La page Configuration de l'interface Promiscuous VLAN privée s'affiche.

6. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :

- **1 ou ID d'unité pour un commutateur empilé :**

- 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
- **ID d'unité pour un commutateur empilé :** Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.

- LAG Seuls les LAG sont affichés.

- **Tous:** Les interfaces physiques et les LAG sont affichés, ou pour une pile de commutateurs, les interfaces physiques de tous les commutateurs de la pile et les LAG sont affichés.

7. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :

- **Pour configurer une interface unique, cochez la case associée au port ou tapez le numéro de port (par exemple g1) dans le champ aller à l'interface et cliquez sur le bouton aller.**
- Pour configurer plusieurs interfaces avec les mêmes paramètres, cochez la case associée à chaque interface.

L'interface que vous sélectionnez doit être configurée en mode Promiscuous (voir [Configurez le mode de port VLAN privé](#) à la page 939).

8. Dans le champ **Promiscuous Primary VLAN**, spécifiez un ID VLAN principal.

Vous pouvez sélectionner un VLAN pour lequel vous avez configuré le type principal (voir [Attribuez un type de VLAN privé à un VLAN](#) à la page 935).

9. Dans le champ **ID VLAN secondaires promiscuous**, spécifiez un ou plusieurs ID VLAN secondaires.

Vous pouvez spécifier les réseaux locaux virtuels pour lesquels vous avez configuré le type isolé ou Communauté, qui sont tous deux des types VLAN secondaires au sein d'un VLAN privé (voir [Attribuez un type de VLAN privé à un VLAN](#) à la page 935).

Vous pouvez spécifier un seul ID VLAN, une plage d'ID VLAN ou une combinaison des deux dans l'ordre, séparés par une virgule (,) :

- Vous pouvez spécifier un ID VLAN individuel, tel que 10.
- Vous pouvez spécifier les valeurs de plage VLAN séparées par un tiret, par exemple, 10-13.
- Vous pouvez spécifier la combinaison des deux séparés par des virgules, par exemple : 12,154043,100010052000

❗ Remarque: Les VLAN ID que vous spécifiez remplacent les VLAN secondaires que vous avez configurés sur la page Private VLAN Association Configuration (voir [Configurez une association VLAN privée avec un VLAN principal et secondaire](#) à la page 936).

10. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

Les champs Operational(s) (VLAN(s) opérationnel(s)) affichent les VLAN primaire et secondaire qui fonctionnent sur l'interface promiscuous.

11. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Interface promiscuous Private VLAN : Supprimez l'interface des VLAN principal et secondaire

Vous pouvez supprimer une interface promiscuous VLAN privée des VLAN principaux et secondaires.

Pour supprimer une interface promiscuous VLAN privée des VLAN principaux et secondaires :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > contrôle du trafic > Private VLAN > Private VLAN Promiscuous interface Configuration**.

La page Configuration de l'interface Promiscuous VLAN privée s'affiche.

6. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :

- **1 ou ID d'unité pour un commutateur empilé :**

- 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
- **ID d'unité pour un commutateur empilé :** Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.

- LAG Seuls les LAG sont affichés.

- **Tous:** Les interfaces physiques et les LAG sont affichés, ou pour une pile de commutateurs, les interfaces physiques de tous les commutateurs de la pile et les LAG sont affichés.

7. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :

- **Pour configurer une interface unique, cochez la case associée au port ou tapez le numéro de port (par exemple g1) dans le champ aller à l'interface et cliquez sur le bouton aller.**
- Pour configurer plusieurs interfaces avec les mêmes paramètres, cochez la case associée à chaque interface.

L'interface que vous sélectionnez doit être configurée en mode Promiscuous (voir [Configurez le mode de port VLAN privé](#) à la page 939).

8. Cliquez sur le bouton **Supprimer**.

Les paramètres sont enregistrés.

Les paramètres sont enregistrés. L'interface est supprimée des VLAN primaire et secondaire.

9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Interface de ligne de réseau promiscuous

Private VLAN : Ajoutez des VLAN principaux et secondaires à la jonction

Si vous configurez le mode de port VLAN privé d'une interface en tant que jonction Promiscuous (voir [Configurez le mode de port VLAN privé](#) à la page 939), vous pouvez ajouter plusieurs configurations VLAN à la jonction. Chaque configuration VLAN se compose d'un VLAN primaire unique et d'un ou plusieurs VLAN secondaires.

Pour ajouter un VLAN principal et des VLAN secondaires à une interface de jonction promiscuous VLAN privée :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > contrôle du trafic > Private VLAN > Configuration de l'interface réseau Promiscuous VLAN privée**.

La page Configuration de l'interface réseau Promiscuous VLAN privée s'affiche.

6. Dans le menu **interface**, sélectionnez une interface ou un lag pour lequel vous avez configuré le mode de port VLAN comme mode de jonction Promiscuous.

Pour plus d'informations sur les modes VLAN des ports, reportez-vous à [Configurez le mode de port VLAN privé](#) à la page 939 la section .

7. Dans le champ **VLAN principal de la jonction Promiscuous**, spécifiez un ID VLAN principal.

Vous pouvez sélectionner un VLAN pour lequel vous avez configuré le type principal (voir [Attribuez un type de VLAN privé à un VLAN](#) à la page 935).

8. Dans le champ **VLAN(s) secondaire(s) de jonction promiscuous**, spécifiez un ou plusieurs ID VLAN secondaires.

Vous pouvez spécifier les réseaux locaux virtuels pour lesquels vous avez configuré le type isolé ou Communauté, qui sont tous deux des types VLAN secondaires au sein d'un VLAN privé (voir [Attribuez un type de VLAN privé à un VLAN](#) à la page 935).

Vous pouvez spécifier un seul ID VLAN, une plage d'ID VLAN ou une combinaison des deux dans l'ordre, séparés par une virgule (,) :

- Vous pouvez spécifier un ID VLAN individuel, tel que 10.
- Vous pouvez spécifier les valeurs de plage VLAN séparées par un tiret, par exemple, 10-13.
- Vous pouvez spécifier la combinaison des deux séparés par des virgules, par exemple : 12,154043,100010052000

❗ Remarque: Les VLAN ID que vous spécifiez remplacent les VLAN secondaires que vous avez configurés sur la page Private VLAN Association Configuration (voir [Configurez une association VLAN privée avec un VLAN principal et secondaire](#) à la page 936).

9. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

Les champs Operational(s) (VLAN(s) opérationnel(s)) affichent les VLAN primaire et secondaire qui fonctionnent sur l'interface de jonction promiscuite.

10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Interface de ligne de réseau promiscuous Private VLAN : Supprimez les VLAN principaux et secondaires de la jonction

Vous pouvez supprimer des VLAN principaux et secondaires d'une interface de jonction promiscuous VLAN privée.

Pour supprimer des VLAN principaux et secondaires d'une interface de jonction promiscuous VLAN privée :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > contrôle du trafic > Private VLAN > Configuration de l'interface réseau Promiscuous VLAN privée**.

La page Configuration de l'interface réseau Promiscuous VLAN privée s'affiche.

6. Dans le menu **interface**, sélectionnez une interface ou un lag pour lequel vous avez configuré le mode de port VLAN comme mode de jonction Promiscuous.

Pour plus d'informations sur les modes VLAN des ports, reportez-vous à [Configurez le mode de port VLAN privé](#) à la page 939 la section .

7. Cochez la case correspondant à la configuration VLAN.
8. Cliquez sur le bouton **Supprimer**.
Les paramètres sont enregistrés.
Les VLAN principal et secondaire sont supprimés de l'interface sélectionnée. Les VLAN eux-mêmes ne sont pas supprimés.
9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Interface de jonction isolée Private VLAN : Ajoutez des VLAN principaux et secondaires à la jonction

Si vous configurez le mode de port VLAN privé d'une interface en tant que jonction isolée (voir [Configurez le mode de port VLAN privé](#) à la page 939), vous pouvez ajouter plusieurs configurations VLAN à la jonction. Chaque configuration VLAN se compose d'un VLAN primaire unique et d'un ou plusieurs VLAN secondaires.

Pour ajouter un VLAN principal et des VLAN secondaires à une interface de jonction isolée VLAN privée :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > contrôle du trafic > Private VLAN > Configuration de l'interface de jonction isolée Private VLAN**.

La page Configuration de l'interface de jonction isolée Private VLAN s'affiche.

6. Dans le menu **interface**, sélectionnez une interface ou un lag pour lequel vous avez configuré le mode de port VLAN en mode réseau isolé.

Pour plus d'informations sur les modes VLAN des ports, reportez-vous à [Configurez le mode de port VLAN privé](#) à la page 939 la section .

7. Dans le champ **VLAN principal de la jonction isolée**, spécifiez un ID VLAN principal. Vous pouvez sélectionner un VLAN pour lequel vous avez configuré le type principal (voir [Attribuez un type de VLAN privé à un VLAN](#) à la page 935).

8. Dans le champ **VLAN(s) secondaire(s) de jonction isolée(s)**, spécifiez un ou plusieurs ID VLAN secondaires.

Vous pouvez spécifier les réseaux locaux virtuels pour lesquels vous avez configuré le type isolé ou Communauté, qui sont tous deux des types VLAN secondaires au sein d'un VLAN privé (voir [Attribuez un type de VLAN privé à un VLAN](#) à la page 935).

Vous pouvez spécifier un seul ID VLAN, une plage d'ID VLAN ou une combinaison des deux dans l'ordre, séparés par une virgule (,) :

- Vous pouvez spécifier un ID VLAN individuel, tel que 10.
- Vous pouvez spécifier les valeurs de plage VLAN séparées par un tiret, par exemple, 10-13.
- Vous pouvez spécifier la combinaison des deux séparés par des virgules, par exemple : 12,154043,100010052000

❗ **Remarque:** Les VLAN ID que vous spécifiez remplacent les VLAN secondaires que vous avez configurés sur la page Private VLAN Association Configuration (voir [Configurez une association VLAN privée avec un VLAN principal et secondaire](#) à la page 936).

9. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

Les champs Operational(s) (VLAN(s) opérationnel(s)) affichent les VLAN principal et secondaire qui fonctionnent sur l'interface de jonction isolée.

10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Interface de jonction isolée Private VLAN : Supprimez les VLAN principaux et secondaires de la jonction

Vous pouvez supprimer des VLAN principaux et secondaires d'une interface de jonction isolée VLAN privée.

Pour supprimer des VLAN principaux et secondaires d'une interface de jonction isolée VLAN privée :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > contrôle du trafic > Private VLAN > Configuration de l'interface de jonction isolée Private VLAN**.

La page Configuration de l'interface de jonction isolée Private VLAN s'affiche.

6. Dans le menu **interface**, sélectionnez une interface ou un lag pour lequel vous avez configuré le mode de port VLAN en mode réseau isolé.

Pour plus d'informations sur les modes VLAN des ports, reportez-vous à [Configurez le mode de port VLAN privé](#) à la page 939 la section .

7. Cochez la case correspondant à la configuration VLAN.

8. Cliquez sur le bouton **Supprimer**.

Les paramètres sont enregistrés.

Les VLAN principal et secondaire sont supprimés de l'interface sélectionnée. Les VLAN eux-mêmes ne sont pas supprimés.

9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez les VLAN natifs et autorisés sur une interface de jonction VLAN privée

Si vous configurez une interface en tant qu'interface promiscuous VLAN privée ou interface de jonction isolée VLAN privée, vous pouvez également autoriser le trafic non balisé à partir d'un VLAN natif sur la même interface de jonction. Par défaut, VLAN 1 est à la fois le par défaut et le VLAN natif, mais vous pouvez configurer un autre VLAN en tant que VLAN natif (voir [Configurez les paramètres du mode de port de commutateur pour les interfaces](#) à la page 319).

Si vous ne spécifiez pas de VLAN natif sur l'interface de jonction privée, tous les paquets non balisés sont supprimés de l'interface de jonction VLAN privée.

Pour configurer des VLAN natifs et autorisés sur une interface de jonction VLAN privée :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > contrôle du trafic > Private VLAN > Configuration de l'interface de jonction VLAN privée**.

La page Configuration de l'interface de jonction VLAN privée s'affiche.

6. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :

- **1 ou ID d'unité pour un commutateur empilé :**

- 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
 - **ID d'unité pour un commutateur empilé** : Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
 - LAG Seuls les LAG sont affichés.
 - **Tous**: Les interfaces physiques et les LAG sont affichés, ou pour une pile de commutateurs, les interfaces physiques de tous les commutateurs de la pile et les LAG sont affichés.
7. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :
- **Pour configurer une interface unique, cochez la case associée au port ou tapez le numéro de port (par exemple g1) dans le champ aller à l'interface et cliquez sur le bouton aller.**
 - Pour configurer plusieurs interfaces avec les mêmes paramètres, cochez la case associée à chaque interface.

L'interface que vous sélectionnez doit être configurée en mode Trunk Promiscuous ou Trunk isolé (voir [Configurez le mode de port VLAN privé](#) à la page 939).

8. Dans le champ **VLAN natif du réseau**, spécifiez un ID VLAN pour un VLAN natif.
- Par défaut, VLAN 1 est à la fois le par défaut et le VLAN natif, mais vous pouvez configurer un autre VLAN en tant que VLAN natif (voir [Configurez les paramètres du mode de port de commutateur pour les interfaces](#) à la page 319).
9. Dans le champ **VLAN de jonction autorisée**, spécifiez un ou plusieurs ID VLAN pour les configurations Private VLAN composées de VLAN principal et de VLAN secondaires.

Vous pouvez spécifier les VLAN pour lesquels vous avez configuré le type Promiscuous, Isolated ou Community dans un VLAN privé (voir [Attribuez un type de VLAN privé à un VLAN](#) à la page 935).

Vous pouvez spécifier un seul ID VLAN, une plage d'ID VLAN ou une combinaison des deux dans l'ordre, séparés par une virgule (,) :

- Vous pouvez spécifier un ID VLAN individuel, tel que 10.
- Vous pouvez spécifier les valeurs de plage VLAN séparées par un tiret, par exemple, 10-13.
- Vous pouvez spécifier la combinaison des deux séparés par des virgules, par exemple : 12,154043,100010052000

❗ Remarque: Les VLAN ID que vous spécifiez remplacent les VLAN secondaires que vous avez configurés sur la page Private VLAN Association Configuration (voir [Configurez une association VLAN privée avec un VLAN principal et secondaire](#) à la page 936).

10. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

Le champ VLAN(s) opérationnel(s) affiche les VLAN qui fonctionnent sur l'interface de jonction VLAN privée.

11. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Storm Control

Une tempête de diffusion est le résultat d'un nombre excessif de messages de diffusion transmis simultanément sur un réseau par un seul port. Les réponses aux messages transférés peuvent surcharger les ressources du réseau, provoquer une expiration du délai d'attente du réseau, ou les deux.

Le commutateur mesure le débit de paquets entrants par port pour les paquets broadcast, multicast, inconnus et unicast et rejette les paquets si le débit dépasse la valeur définie. Vous activez storm control par interface, en définissant le type de paquet et la vitesse à laquelle les paquets sont transmis.

Configurer les paramètres storm control globaux

Les paramètres storm control globaux s'appliquent à tous les ports. Après avoir configuré les paramètres globaux, vous pouvez spécifier les paramètres storm control pour un ou plusieurs ports.

Pour configurer les paramètres storm control globaux :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > contrôle du trafic > storm control > Configuration globale storm control**.

La page Configuration globale storm control s'affiche.

Les trois paramètres suivants vous permettent d'activer ou de désactiver globalement chaque type de paquet à débit limité sur tous les ports. Pour plus d'informations sur les ports individuels, reportez-vous à [Configurez les paramètres storm control pour un ou plusieurs ports](#) à la page 961 la section .

6. Configurez les paramètres storm control en sélectionnant un bouton radio :
 - **Diffusion storm control tout** : Activer ou désactiver cette option :
 - Activer. Si le trafic de diffusion sur un port dépasse le seuil configuré, le commutateur rejette le trafic de diffusion. La valeur par défaut est Activer.
 - Désactiver : Broadcast storm control est désactivé sur tous les ports.
 - **Multicast storm control All** : Activer ou désactiver cette option :
 - Activer. Si le trafic multicast sur un port dépasse le seuil configuré, le commutateur rejette le trafic multicast.
 - Désactiver : Le protocole storm control multicast est désactivé sur tous les ports. La valeur par défaut est désactiver.
 - **Unicast storm control inconnu tous** : Activer ou désactiver cette option :
 - Activer. Si le trafic unicast inconnu sur un port dépasse le seuil configuré, le commutateur rejette le trafic unicast inconnu.
 - Désactiver : Le storm control Unicast inconnu est désactivé sur tous les ports. La valeur par défaut est désactiver.
7. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez les paramètres storm control pour un ou plusieurs ports

Vous pouvez spécifier des paramètres storm control pour un ou plusieurs ports.

Pour configurer le contrôle de flux pour un ou plusieurs ports :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > contrôle du trafic > storm control > Configuration de l'interface storm control**.

La page Configuration de l'interface storm control s'affiche.

6. Si une pile est configurée, indiquez si vous souhaitez afficher les interfaces physiques d'un commutateur ou de tous les commutateurs de la pile :

- **ID d'unité pour un commutateur empilé** : Les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
Si aucune pile de commutateurs n'est configurée, la seule option est l'ID d'unité 1.
 - **Tous** : Les interfaces physiques de tous les commutateurs de la pile sont affichées.
Si aucune pile de commutateurs n'est configurée, l'option tous n'a aucun effet.
7. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :
- **Pour configurer une interface unique, cochez la case associée au port ou tapez le numéro de port (par exemple g1) dans le champ aller à l'interface et cliquez sur le bouton aller.**
 - Pour configurer plusieurs interfaces avec les mêmes paramètres, cochez la case associée à chaque interface.
 - Pour configurer toutes les interfaces avec les mêmes paramètres, cochez la case dans la ligne d'en-tête.
8. Configurez les paramètres suivants pour les tempêtes de diffusion :
- **Mode de récupération** Activer ou désactiver cette option pour le trafic de diffusion :
 - Activer. Si le trafic de diffusion dépasse le seuil configuré, le port rejette le trafic de diffusion. La valeur par défaut est Activer.
 - Désactiver : Si le trafic de diffusion dépasse le seuil configuré, la diffusion n'est pas rejetée.
 - **Type de niveau de récupération** : Spécifiez le niveau de restauration dans le champ **niveau de restauration** en pourcentage de la vitesse de liaison du port ou en paquets par seconde :
 - **Pourcentage** : Le niveau de récupération est exprimé en pourcentage de la vitesse de liaison.
 - **pps** : Le niveau de récupération est exprimé en paquets par seconde (PPS).
 - **Niveau de récupération** : Spécifiez le seuil auquel le storm control de diffusion est activé. Par défaut, le niveau de récupération est de 5 % de la vitesse de liaison du port de 5 PPS.
 - **Action de contrôle** : Spécifiez l'une des actions suivantes :
 - **Aucun** : Aucune autre mesure n'est prise. Il s'agit de l'option par défaut.
 - **Piège** : Si le trafic de diffusion dépasse le seuil configuré, une interruption est envoyée.
 - **Shutdown** (Arrêter) : Si le trafic de diffusion dépasse le seuil configuré, le port est arrêté.
9. Configurez les paramètres suivants pour les tempêtes de multidiffusion :

- Mode de récupération Activer ou désactiver cette option pour le trafic multicast :
 - Activer. Si le trafic multicast dépasse le seuil configuré, le port rejette le trafic multicast. La valeur par défaut est Activer.
 - Désactiver : Si le trafic de multidiffusion dépasse le seuil configuré, la multidiffusion n'est pas rejetée.
- **Type de niveau de récupération** : Spécifiez le niveau de restauration dans le champ **niveau de restauration** en pourcentage de la vitesse de liaison du port ou en paquets par seconde :
 - **Pourcentage** : Le niveau de récupération est exprimé en pourcentage de la vitesse de liaison.
 - **pps** : Le niveau de récupération est exprimé en paquets par seconde (PPS).
- **Niveau de récupération** : Spécifiez le seuil auquel le storm control multicast est activé. Par défaut, le niveau de récupération est de 5 % de la vitesse de liaison du port de 5 PPS.
- **Action de contrôle** : Spécifiez l'une des actions suivantes :
 - Aucun : Aucune autre mesure n'est prise. Il s'agit de l'option par défaut.
 - **Piège** : Si le trafic multicast dépasse le seuil configuré, une interruption est envoyée.
 - **Shutdown** (Arrêter) : Si le trafic multicast dépasse le seuil configuré, le port est arrêté.

10. Configurez les paramètres suivants pour les tempêtes de monodiffusion :

- Mode de récupération Activer ou désactiver cette option pour le trafic monodiffusion :
 - Activer. Si le trafic de monodiffusion dépasse le seuil configuré, le port rejette le trafic de monodiffusion. La valeur par défaut est Activer.
 - Désactiver : Si le trafic de monodiffusion dépasse le seuil configuré, la monodiffusion n'est pas supprimée.
- **Type de niveau de récupération** : Spécifiez le niveau de restauration dans le champ **niveau de restauration** en pourcentage de la vitesse de liaison du port ou en paquets par seconde :
 - **Pourcentage** : Le niveau de récupération est exprimé en pourcentage de la vitesse de liaison.
 - **pps** : Le niveau de récupération est exprimé en paquets par seconde (PPS).
- **Niveau de récupération** : Spécifiez le seuil auquel le storm control monodiffusion est activé. Par défaut, le niveau de récupération est de 5 % de la vitesse de liaison du port de 5 PPS.
- **Action de contrôle** : Spécifiez l'une des actions suivantes :

- Aucun : Aucune autre mesure n'est prise. Il s'agit de l'option par défaut.
- **Piège** : Si le trafic de monodiffusion dépasse le seuil configuré, une interruption est envoyée.
- **Shutdown** (Arrêter) : Si le trafic de monodiffusion dépasse le seuil configuré, le port est arrêté.

11. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

12. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Protocole DHCP Snooping

DHCP Snooping est une fonctionnalité qui fournit la sécurité en filtrant les messages DHCP non fiables et en créant et en maintenant une table de liaison DHCP Snooping. Un message non approuvé est un message reçu de l'extérieur du réseau ou du pare-feu et qui peut provoquer des attaques de trafic au sein de votre réseau. La table de liaison DHCP Snooping contient l'adresse MAC, l'adresse IP, la durée de bail, le type de liaison, le numéro VLAN et les informations d'interface correspondant aux interfaces locales non fiables d'un commutateur. Une interface non approuvée est une interface configurée pour recevoir des messages provenant de l'extérieur du réseau ou du pare-feu. Une interface approuvée est une interface configurée pour recevoir uniquement des messages provenant du réseau.

La surveillance DHCP agit comme un pare-feu entre les hôtes non approuvés et les serveurs DHCP. L'information permet également de différencier les interfaces non fiables connectées à l'utilisateur final des interfaces fiables connectées au serveur DHCP ou à un autre commutateur.

Activez la surveillance DHCP pour le commutateur

Vous pouvez activer globalement la surveillance DHCP pour le commutateur.

Pour activer globalement la surveillance DHCP pour le commutateur :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > contrôle > surveillance DHCP > Configuration globale**.

La page Configuration globale s'affiche.

6. Sélectionnez le bouton radio **Activer** le mode de surveillance DHCP.

La valeur par défaut est désactiver.

7. Pour activer la vérification de l'adresse MAC de l'expéditeur pour la surveillance DHCP, laissez le bouton radio **Activer** la validation de l'adresse MAC sélectionné.

La valeur par défaut est Activer.

Lorsque la validation de l'adresse MAC est activée, le commutateur vérifie les paquets reçus sur une interface non sécurisée pour vérifier que l'adresse MAC et l'adresse matérielle du client DHCP correspondent. Si les adresses ne correspondent pas, le commutateur abandonne le paquet.

8. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Activez la surveillance DHCP pour un VLAN

Vous pouvez activer la surveillance DHCP sur un ou plusieurs VLAN.

Pour activer igmp snooping pour un VLAN :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.
Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.
4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **sécurité > contrôle > surveillance DHCP > Configuration globale** .
La page Configuration globale s'affiche.
6. Dans le champ **ID VLAN**, saisissez un ID VLAN.
7. Dans le menu **DHCP Snooping mode (mode de surveillance DHCP)**, sélectionnez **Enable(Activer)**.
8. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
L'ID VLAN s'affiche dans le tableau de configuration VLAN.
9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez les paramètres de l'interface de surveillance DHCP.

Vous pouvez afficher et configurer chaque port en tant que port approuvé ou non approuvé. Toutes les réponses DHCP reçues sur un port approuvé sont transmises. Si un port est configuré comme non approuvé, toutes les réponses DHCP (ou BootP) reçues sur ce port sont ignorées.

Pour configurer les paramètres de l'interface de surveillance DHCP :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > contrôle > surveillance DHCP > Configuration de l'interface**.

La page Configuration de l'interface s'affiche.

6. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :

- **1 ou ID d'unité pour un commutateur empilé :**

- 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
 - **ID d'unité pour un commutateur empilé** : Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
 - LAG Seuls les LAG sont affichés.
 - **Tous**: Les interfaces physiques et les LAG sont affichés, ou pour une pile de commutateurs, les interfaces physiques de tous les commutateurs de la pile et les LAG sont affichés.
7. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :
- **Pour configurer une interface unique, cochez la case associée au port ou tapez le numéro de port (par exemple g1) dans le champ aller à l'interface et cliquez sur le bouton aller.**
 - Pour configurer plusieurs interfaces avec les mêmes paramètres, cochez la case associée à chaque interface.
 - Pour configurer toutes les interfaces avec les mêmes paramètres, cochez la case dans la ligne d'en-tête.
8. Dans le menu **Trust mode**, sélectionnez le mode Trust :
- **Désactivé** : L'interface est considérée comme non fiable et pourrait potentiellement être utilisée pour lancer une attaque réseau. Les messages du serveur DHCP sont vérifiés par rapport à la base de données de liaisons. Sur les ports non approuvés, la surveillance DHCP applique les règles de sécurité suivantes :
 - Les paquets DHCP d'un serveur DHCP sont abandonnés.
 - Les messages DHCP sont abandonnés si l'adresse MAC se trouve dans la base de données de surveillance mais que l'interface de la liaison est autre que l'interface où le message a été reçu.
 - Les paquets DHCP sont abandonnés si l'adresse MAC source ne correspond pas à l'adresse matérielle du client et si la validation de l'adresse MAC est globalement activée.
 - **Sous tension** L'interface est considérée comme fiable et transfère les messages du serveur DHCP sans validation.
9. Dans le menu **paquets non valides**, sélectionnez le mode de consignation des paquets.
- Lorsqu'elle est activée, la fonction de surveillance DHCP génère un message de journal lorsqu'un paquet non valide est reçu et abandonné par l'interface.
10. Dans le champ **limite de débit (PPS)**, spécifiez la valeur limite de débit pour la surveillance DHCP.

Si le débit entrant de paquets DHCP par seconde dépasse l'intervalle de rafale configuré par seconde, le port s'arrête. Si la limite de débit est None (aucun) (valeur par défaut), l'intervalle de rafale n'est pas non plus applicable et la limitation de débit est désactivée.

11. Dans le champ **intervalle de rafale (sec)**, spécifiez l'intervalle de rafale en secondes pour la limitation de débit sur l'interface.

Si la limite de débit est N/A, l'intervalle de rafale n'est pas applicable.

12. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

13. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Ajoutez une liaison DHCP statique et affichez ou effacez les liaisons DHCP dynamiques

Vous pouvez ajouter une liaison statique dans la base de données DHCP Snooping bindings et afficher ou effacer les liaisons dynamiques dans la table des liaisons.

Pour ajouter une liaison DHCP statique et afficher ou effacer les liaisons dynamiques :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > contrôle > surveillance DHCP > Configuration de liaison**.

La page Configuration de la liaison s'affiche.

6. Dans le menu **interface**, sélectionnez l'interface.
7. Dans le champ **adresse MAC**, spécifiez l'adresse MAC de la liaison à ajouter.
C'est la clé de la base de données de liaison.
8. Dans le menu **VLAN ID**, sélectionnez l'ID du VLAN.
9. Dans le champ **adresse IP**, spécifiez l'adresse IP de la liaison à ajouter.
10. Cliquez sur le bouton **Add** (Ajouter).

L'entrée de liaison DHCP Snooping est ajoutée à la base de données.

Le tableau Configuration de la liaison dynamique affiche des informations sur les liaisons DHCP apprises sur chaque interface sur laquelle la surveillance DHCP est activée. Le tableau suivant décrit les informations de liaison dynamique.

Champ	Description
Interface	Interface sur laquelle le message client DHCP a été reçu.
Adresse MAC	Adresse MAC associée au client DHCP qui a envoyé le message. C'est la clé de la base de données de liaison.
Identifiant VLAN	ID VLAN de l'interface client.
Adresse IP	Adresse IP attribuée au client par le serveur DHCP.
Durée du bail :	Durée de bail de l'adresse IP restante pour le client.

11. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

12. Pour effacer toutes les liaisons dynamiques du tableau Configuration de liaison dynamique, cliquez sur le bouton **Effacer**.
13. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimez une liaison DHCP statique

Vous pouvez supprimer une liaison statique de la base de données DHCP Snooping bindings.

Pour supprimer une liaison DHCP statique :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.
Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.
4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **sécurité > contrôle > surveillance DHCP > Configuration de liaison**.
La page Configuration de la liaison s'affiche.
6. Dans le tableau Configuration de la liaison statique, cochez la case de la liaison statique.

7. Cliquez sur le bouton **Supprimer**.

L'entrée de liaison DHCP Snooping est supprimée de la base de données.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez les paramètres persistants de surveillance DHCP

Vous pouvez configurer l'emplacement persistant de la base de données des liaisons de surveillance DHCP. La base de données de liaisons peut être stockée localement sur le commutateur ou sur un périphérique distant du réseau. Le commutateur doit pouvoir atteindre l'adresse IP du périphérique distant pour envoyer des liaisons à une base de données distante.

Pour configurer les paramètres persistants de surveillance DHCP :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > contrôle > surveillance DHCP > Configuration persistante**.

La page Configuration permanente s'affiche.

6. Spécifiez l'emplacement de la base de données des liaisons de surveillance DHCP.

- Local La table de reliure est stockée localement sur le commutateur.
- Distant : La table de liaison est stockée sur un serveur TFTP distant.

Si la base de données est stockée sur un serveur distant, spécifiez les informations suivantes :

- Adresse IP distante Spécifiez l'adresse IP du serveur TFTP.
- **Nom du fichier distant** : Spécifiez le nom de fichier de la base de données DHCP Snooping bindings dans laquelle les bindings sont stockés.

7. Dans le champ **délai d'écriture**, spécifiez le temps d'attente du commutateur après l'écriture des informations de liaison dans le stockage persistant.

Le délai permet au commutateur de collecter autant d'entrées que possible (nouvelles et supprimées) avant de les écrire dans le fichier persistant. Vous pouvez spécifier de 15 à 86400 secondes. Par défaut, le délai est de 300 secondes.

8. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Afficher ou effacer les statistiques de surveillance DHCP

Vous pouvez afficher et effacer les statistiques par interface sur les messages DHCP filtrés par la fonction de surveillance DHCP sur les interfaces non fiables.

Pour afficher ou effacer les statistiques de surveillance DHCP :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > contrôle > surveillance DHCP > statistiques**.

La page statistiques s'affiche.

6. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :

- **1 ou ID d'unité pour un commutateur empilé :**
 - 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
 - **ID d'unité pour un commutateur empilé :** Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
- **LAG** Seuls les LAG sont affichés.
- **Tous:** Les interfaces physiques et les LAG sont affichés, ou pour une pile de commutateurs, les interfaces physiques de tous les commutateurs de la pile et les LAG sont affichés.

7. Cliquez sur le bouton **Effacer** pour effacer toutes les statistiques d'interface.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les statistiques de surveillance DHCP.

Table 176 : Informations statistiques DHCP Snooping

Champ	Description
Échecs de vérification MAC	Nombre de messages DHCP abandonnés parce que l'adresse MAC source et l'adresse matérielle du client ne correspondent pas. La vérification de l'adresse MAC est effectuée uniquement si informatique est activé globalement.
Incohérence IFC client	Nombre de paquets abandonnés par la surveillance DHCP car l'interface et le VLAN sur lesquels le paquet a été reçu ne correspondent pas à l'interface du client et aux informations VLAN stockées dans la base de données de liaison.
Messages du serveur DHCP	Nombre de messages de serveur DHCP abandonnés sur un port non approuvé.

Surveillance DHCPv6

La surveillance DHCPv6 est une fonctionnalité qui fournit la sécurité en filtrant les messages DHCPv6 non fiables et en construisant et en maintenant une table de liaison de surveillance DHCPv6. Un message non approuvé est un message reçu de l'extérieur du réseau ou du pare-feu et qui peut provoquer des attaques de trafic au sein de votre réseau. La table de liaison de surveillance DHCPv6 contient l'adresse MAC, l'adresse IP, la durée de bail, le type de liaison, le numéro VLAN et les informations d'interface correspondant aux interfaces locales non fiables d'un commutateur. Une interface non approuvée est une interface configurée pour recevoir des messages provenant de l'extérieur du réseau ou du pare-feu. Une interface approuvée est une interface configurée pour recevoir uniquement des messages provenant du réseau.

La surveillance DHCPv6 agit comme un pare-feu entre les hôtes non approuvés et les serveurs DHCPv6. informatique fournit également un moyen de différencier les interfaces non approuvées connectées à l'utilisateur final et les interfaces approuvées connectées au serveur DHCPv6 ou à un autre commutateur.

Activez la surveillance DHCPv6 pour le commutateur

Vous pouvez activer globalement la surveillance DHCPv6 pour le commutateur.

Pour activer globalement la surveillance DHCPv6 pour le commutateur :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > contrôle > surveillance DHCPv6 > Configuration globale**

La page Configuration globale s'affiche.

6. Sélectionnez le bouton radio **Activer** le mode de surveillance DHCPv6.

La valeur par défaut est désactiver.

7. Pour activer la vérification de l'adresse MAC de l'expéditeur pour la surveillance DHCPv6, laissez le bouton radio **Activer la validation de l'adresse MAC** sélectionné.

La valeur par défaut est Activer.

Lorsque la validation de l'adresse MAC est activée, le commutateur vérifie les paquets reçus sur une interface non approuvée pour vérifier que l'adresse MAC et l'adresse matérielle du client DHCPv6 correspondent. Si les adresses ne correspondent pas, le commutateur abandonne le paquet.

8. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Activez la surveillance DHCPv6 pour un VLAN

Vous pouvez activer la surveillance DHCPv6 sur un ou plusieurs VLAN.

Pour activer igmp snooping pour un VLAN :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > contrôle > surveillance DHCPv6 > Configuration globale**.

La page Configuration globale s'affiche.

6. Dans le champ **ID VLAN**, saisissez un ID VLAN.

7. Dans le menu **mode de surveillance DHCPv6**, sélectionnez **Activer**.

8. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

L'ID VLAN s'affiche dans le tableau de configuration VLAN.

9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez les paramètres de l'interface de surveillance DHCP.

Vous pouvez afficher et configurer chaque port en tant que port approuvé ou non approuvé. Toutes les réponses DHCPv6 reçues sur un port approuvé sont transmises. Si un port est configuré comme non approuvé, toutes les réponses DHCPv6 (ou BootP) reçues sur ce port sont ignorées.

Pour configurer les paramètres de l'interface de surveillance DHCPv6 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > contrôle > surveillance DHCPv6 > Configuration de l'interface**.

La page Configuration de l'interface s'affiche.

6. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :
 - **1 ou ID d'unité pour un commutateur empilé :**
 - 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
 - **ID d'unité pour un commutateur empilé :** Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
 - LAG Seuls les LAG sont affichés.
 - **Tous:** Les interfaces physiques et les LAG sont affichés, ou pour une pile de commutateurs, les interfaces physiques de tous les commutateurs de la pile et les LAG sont affichés.
7. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :
 - **Pour configurer une interface unique, cochez la case associée au port ou tapez le numéro de port (par exemple g1) dans le champ aller à l'interface et cliquez sur le bouton aller.**
 - Pour configurer plusieurs interfaces avec les mêmes paramètres, cochez la case associée à chaque interface.
 - Pour configurer toutes les interfaces avec les mêmes paramètres, cochez la case dans la ligne d'en-tête.
8. Dans le menu **Trust mode**, sélectionnez le mode Trust :
 - **Désactivé :** L'interface est considérée comme non fiable et pourrait potentiellement être utilisée pour lancer une attaque réseau. Les messages du serveur DHCPv6 sont vérifiés par rapport à la base de données des liaisons. Sur les ports non approuvés, la surveillance DHCPv6 applique les règles de sécurité suivantes :
 - Les paquets DHCPv6 d'un serveur DHCPv6 sont abandonnés.
 - Les messages DHCPv6 sont supprimés si l'adresse MAC se trouve dans la base de données de surveillance mais que l'interface de la liaison est autre que l'interface où le message a été reçu.
 - Les paquets DHCPv6 sont abandonnés si l'adresse MAC source ne correspond pas à l'adresse matérielle du client et si la validation de l'adresse MAC est globalement activée.
 - **Sous tension** L'interface est considérée comme fiable et transfère les messages du serveur DHCPv6 sans validation.

9. Dans le menu **paquets non valides**, sélectionnez le mode de consignation des paquets.
Lorsqu'elle est activée, la fonction de surveillance DHCPv6 génère un message de journal lorsqu'un paquet non valide est reçu et abandonné par l'interface.
10. Dans le champ **limite de débit (PPS)**, spécifiez la valeur limite de débit pour la surveillance DHCPv6.
Si le débit entrant de paquets DHCPv6 par seconde dépasse l'intervalle de rafale configuré par seconde, le port s'arrête. Si la limite de débit est None (aucun) (valeur par défaut), l'intervalle de rafale n'est pas non plus applicable et la limitation de débit est désactivée.
11. Dans le champ **intervalle de rafale (sec)**, spécifiez l'intervalle de rafale en secondes pour la limitation de débit sur l'interface.
Si la limite de débit est N/A, l'intervalle de rafale n'est pas applicable.
12. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
13. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Ajoutez une liaison DHCPv6 statique et affichez ou effacez les liaisons DHCPv6 dynamiques

Vous pouvez ajouter une liaison statique dans la base de données des liaisons de surveillance DHCPv6 et afficher ou effacer les liaisons dynamiques dans la table des liaisons.

Pour ajouter une liaison DHCPv6 statique et afficher ou effacer les liaisons dynamiques :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **sécurité > contrôle > surveillance DHCPv6 > Configuration de liaison**.

La page Configuration de la liaison s'affiche.

6. Dans le menu **interface**, sélectionnez l'interface.
7. Dans le champ **adresse MAC**, spécifiez l'adresse MAC de la liaison à ajouter.
C'est la clé de la base de données de liaison.
8. Dans le menu **VLAN ID**, sélectionnez l'ID du VLAN.
9. Dans le champ **adresse IPv6**, spécifiez l'adresse IPv6 pour la liaison à ajouter.
10. Cliquez sur le bouton **Add** (Ajouter).

L'entrée de liaison de surveillance DHCPv6 est ajoutée à la base de données.

Le tableau Configuration de liaison dynamique affiche des informations sur les liaisons DHCPv6 apprises sur chaque interface sur laquelle la surveillance DHCPv6 est activée. Le tableau suivant décrit les informations de liaison dynamique.

Champ	Description
Interface	Interface sur laquelle le message client DHCPv6 a été reçu.
Adresse MAC	Adresse MAC associée au client DHCPv6 qui a envoyé le message. C'est la clé de la base de données de liaison.
Identifiant VLAN	ID VLAN de l'interface client.
Adresse IPv6	Adresse IPv6 attribuée au client par le serveur DHCPv6.
Durée du bail :	Durée de bail de l'adresse IP restante pour le client.

11. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

12. Pour effacer toutes les liaisons dynamiques du tableau Configuration de liaison dynamique, cliquez sur le bouton **Effacer**.
13. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimez une liaison DHCPv6 statique

Vous pouvez supprimer une liaison statique de la base de données des liaisons de surveillance DHCPv6.

Pour supprimer une liaison DHCPv6 statique :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.
Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.
4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **sécurité > contrôle > surveillance DHCPv6 > Configuration de liaison** .
La page Configuration de la liaison s'affiche.
6. Dans le tableau Configuration de la liaison statique, cochez la case de la liaison statique.

7. Cliquez sur le bouton **Supprimer**.

L'entrée de liaison de surveillance DHCPv6 est supprimée de la base de données.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurer les paramètres persistants de surveillance DHCPv6

Vous pouvez configurer l'emplacement persistant de la base de données des liaisons de surveillance DHCPv6. La base de données de liaisons peut être stockée localement sur le commutateur ou sur un périphérique distant du réseau. Le commutateur doit pouvoir atteindre l'adresse IP du périphérique distant pour envoyer des liaisons à une base de données distante.

Pour configurer les paramètres persistants de surveillance DHCPv6 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > contrôle > surveillance DHCPv6 > Configuration persistante**.

La page Configuration permanente s'affiche.

6. Spécifiez l'emplacement de la base de données des liaisons de surveillance DHCPv6.

- Local La table de reliure est stockée localement sur le commutateur.
- Distant : La table de liaison est stockée sur un serveur TFTP distant.

Si la base de données est stockée sur un serveur distant, spécifiez les informations suivantes :

- Adresse IP distante Spécifiez l'adresse IP du serveur TFTP.
- **Nom du fichier distant** : Spécifiez le nom de fichier de la base de données de liaisons de surveillance DHCPv6 dans laquelle les liaisons sont stockées.

7. Dans le champ **délai d'écriture**, spécifiez le temps d'attente du commutateur après l'écriture des informations de liaison dans le stockage persistant.

Le délai permet au commutateur de collecter autant d'entrées que possible (nouvelles et supprimées) avant de les écrire dans le fichier persistant. Vous pouvez spécifier de 15 à 86400 secondes. Par défaut, le délai est de 300 secondes.

8. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Afficher ou effacer les statistiques de surveillance DHCPv6

Vous pouvez afficher et effacer les statistiques par interface sur les messages DHCPv6 filtrés par la fonctionnalité de surveillance DHCPv6 sur les interfaces non fiables.

Pour afficher ou effacer les statistiques de surveillance DHCPv6 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > contrôle > surveillance DHCPv6 > statistiques**.

La page statistiques s'affiche.

6. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :

- **1 ou ID d'unité pour un commutateur empilé :**
 - 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
 - **ID d'unité pour un commutateur empilé :** Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
- **LAG** Seuls les LAG sont affichés.
- **Tous:** Les interfaces physiques et les LAG sont affichés, ou pour une pile de commutateurs, les interfaces physiques de tous les commutateurs de la pile et les LAG sont affichés.

7. Cliquez sur le bouton **Effacer** pour effacer toutes les statistiques d'interface.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les statistiques de surveillance DHCPv6.

Table 177 : Informations statistiques de surveillance DHCPv6

Champ	Description
Échecs de vérification MAC	Nombre de messages DHCPv6 abandonnés parce que l'adresse MAC source et l'adresse matérielle du client ne correspondaient pas. La vérification de l'adresse MAC est performed uniquement si informatique est activé globalement.
Incohérence IFC client	Nombre de paquets abandonnés par la surveillance DHCPv6 car l'interface et le VLAN sur lesquels le paquet a été reçu ne correspondent pas à l'interface du client et aux informations VLAN stockées dans la base de données de liaison.
MSG serveur DHCPv6	Nombre de messages du serveur DHCPv6 qui ont été abandonnés sur un port non approuvé.

Interfaces IP source Guard

Vous pouvez configurer IP source Guard (IPSG) sur des interfaces individuelles. IPSG est une fonction de sécurité qui filtre les paquets IP en fonction de l'ID source. Cette fonctionnalité aide à protéger le réseau contre les attaques qui utilisent l'usurpation d'adresse IP pour compromettre ou submerger le réseau. L'ID source peut être soit l'adresse IP source, soit une combinaison d'une adresse IP source et d'une adresse MAC source, appelée paire. La base de données des liaisons de surveillance DHCP, ainsi que les entrées IPSG de la base de données, identifient les ID source autorisés.

Si vous activez IPSG sur un port sur lequel la surveillance DHCP est désactivée ou sur lequel la surveillance DHCP est activée mais que le port n'est pas fiable, tout le trafic IP reçu sur ce port est abandonné. En outre, IPSG interagit avec la sécurité des ports (voir [Sécurité portuaire](#) à la page 919) pour appliquer l'adresse MAC source dans les paquets entrants. La sécurité des ports contrôle la façon dont les adresses MAC sources sont apprises dans la base de données de transfert de couche 2 (la table des adresses MAC). Si un port reçoit une trame avec une adresse MAC source précédemment non apprise, la sécurité du port utilise IPSG pour déterminer si l'adresse MAC appartient à une liaison valide.

Configurer la protection source IP sur une interface

Vous pouvez configurer IP source Guard sur des interfaces individuelles.

Pour configurer IP source Guard sur une interface :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > contrôle > IP source Guard > Configuration de l'interface**

La page Configuration de l'interface s'affiche.

6. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :

- **1 ou ID d'unité pour un commutateur empilé :**
 - 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
 - **ID d'unité pour un commutateur empilé :** Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
- **LAG** Seuls les LAG sont affichés.
- **Tous:** Les interfaces physiques et les LAG sont affichés, ou pour une pile de commutateurs, les interfaces physiques de tous les commutateurs de la pile et les LAG sont affichés.

7. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :

- **Pour configurer une interface unique, cochez la case associée au port ou tapez le numéro de port (par exemple g1) dans le champ aller à l'interface et cliquez sur le bouton aller.**
 - Pour configurer plusieurs interfaces avec les mêmes paramètres, cochez la case associée à chaque interface.
 - Pour configurer toutes les interfaces avec les mêmes paramètres, cochez la case dans la ligne d'en-tête.
8. Dans le menu **IPSG mode**, spécifiez le mode d'administration d'IPSG sur l'interface :
- Activer. IPSG est activé sur l'interface. L'adresse IP de la source n'est pas dans la base de données de liaison DHCP Snooping, les paquets ne sont pas transférés.
 - Désactiver : IPSG est désactivé sur l'interface. La valeur par défaut est désactiver.
9. Dans le menu **IPSG Port Security**, spécifiez le mode d'administration de la sécurité du port IPSG sur l'interface :
- Activer. La sécurité du port IPSG est activée sur l'interface. Les paquets ne sont pas transférés si l'adresse MAC de la source ne se trouve pas dans la table de la base de données de transfert ou dans la base de données de liaison de surveillance DHCP. Pour appliquer le filtrage basé sur l'adresse MAC, vous devez également configurer les fonctionnalités suivantes :
 - Activez la sécurité des ports globalement (voir [Configurez le mode de sécurité du port global](#) à la page 919).
 - Activez la sécurité des ports sur l'interface (voir [Configurer une interface de sécurité de port](#) à la page 920).
 - Désactiver : La sécurité du port IPSG est désactivée sur l'interface. La valeur par défaut est désactiver.
10. Cliquez sur le bouton **Apply** (Appliquer).
- Les paramètres sont enregistrés.
11. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Ajoutez une liaison IP source Guard statique et affichez ou effacez les liaisons IP source Guard dynamiques

Vous pouvez ajouter une liaison statique dans la base de données de liaisons IPSG (IP source Guard) et afficher ou effacer les liaisons dynamiques dans la table de liaisons.

Pour ajouter une liaison IPSG statique et afficher ou effacer les liaisons IPSG dynamiques :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > contrôle > IP source Guard > Configuration de liaison** .

La page Configuration de la liaison s'affiche.

6. Dans le menu **interface**, sélectionnez l'interface.

7. Dans le champ **adresse MAC**, spécifiez l'adresse MAC de la liaison à ajouter.

C'est la clé de la base de données de liaison.

8. Dans le menu **VLAN ID**, sélectionnez l'ID du VLAN.

9. Dans le champ **adresse IP**, spécifiez l'adresse IP de la liaison à ajouter.

10. Cliquez sur le bouton **Add** (Ajouter).

L'entrée de liaison statique IPSG est ajoutée à la base de données.

Le champ type de filtre s'affiche si IPSG est configuré pour fonctionner avec l'adresse IP source uniquement ou, si la sécurité du port est également activée pour IPSG, avec l'adresse IP source et l'adresse MAC.

Le tableau Configuration de la liaison dynamique affiche des informations sur les liaisons IPSG apprises sur chaque interface sur laquelle IPSG est activé. Le tableau suivant décrit les informations de liaison dynamique.

Champ	Description
Interface	Interface sur laquelle la liaison source IPSG a été apprise.
Adresse MAC	Adresse MAC associée au périphérique source IPSG. C'est la clé de la base de données binding.
Identifiant VLAN	ID VLAN de l'interface du périphérique source IPSG.
Adresse IP	Adresse IP du périphérique source IPSG.
Type de filtre	Type de filtre utilisé sur l'interface du commutateur. IPSG est configuré pour fonctionner avec l'adresse IP source uniquement ou, si la sécurité du port est également activée pour IPSG, avec l'adresse IP source et l'adresse MAC.

11. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.
12. Pour effacer toutes les liaisons dynamiques du tableau Configuration de liaison dynamique, cliquez sur le bouton **Effacer**.
13. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimez une liaison statique de la protection de la source IP

Vous pouvez supprimer une liaison statique de la base de données de liaisons IPSG (IP source Guard).

Pour supprimer une liaison IPSG statique :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > contrôle > IP source Guard > Configuration de liaison**.

La page Configuration de la liaison s'affiche.

6. Dans le tableau Configuration de la liaison statique, cochez la case de la liaison statique.

7. Cliquez sur le bouton **Supprimer**.

L'entrée de liaison IPSG est supprimée de la base de données.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Interfaces de protection source IPv6

Vous pouvez configurer IPv6 source Guard (IPv6SG) sur des interfaces individuelles. IPv6SG est une fonction de sécurité qui filtre les paquets IPv6 en fonction de l'ID source. Cette fonctionnalité aide à protéger le réseau contre les attaques qui utilisent l'usurpation d'adresse IPv6 pour compromettre ou submerger le réseau. L'ID source peut être soit l'adresse IPv6 source, soit une combinaison d'une adresse IPv6 source et d'une adresse MAC source, appelée paire. La base de données des liaisons de surveillance DHCP, ainsi que les entrées IPv6SG de la base de données, identifient les ID source autorisés.

Si vous activez IPv6SG sur un port sur lequel la surveillance DHCP est désactivée ou sur lequel la surveillance DHCP est activée mais que le port n'est pas fiable, tout le trafic IPv6 reçu sur ce port est abandonné. En outre, IPv6SG interagit avec la sécurité des ports (voir [Sécurité portuaire](#) à la page 919) pour appliquer l'adresse MAC source dans les paquets entrants. La sécurité des ports contrôle la façon dont les adresses MAC sources sont apprises dans la base de données de transfert de couche 2 (la table des adresses MAC). Si un port reçoit une trame avec une adresse MAC source précédemment

non apprise, la sécurité du port utilise IPv6SG pour déterminer si l'adresse MAC appartient à une liaison valide.

Configurer la protection source IPv6 sur une interface

Vous pouvez configurer la protection source IPv6 sur des interfaces individuelles.

Pour configurer la protection source IPv6 sur une interface :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > contrôle > IPv6 source Guard > Configuration de l'interface**.

La page Configuration de l'interface s'affiche.

6. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :

- **1 ou ID d'unité pour un commutateur empilé :**

- 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
 - **ID d'unité pour un commutateur empilé** : Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
 - LAG Seuls les LAG sont affichés.
 - **Tous**: Les interfaces physiques et les LAG sont affichés, ou pour une pile de commutateurs, les interfaces physiques de tous les commutateurs de la pile et les LAG sont affichés.
7. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :
- **Pour configurer une interface unique, cochez la case associée au port ou tapez le numéro de port (par exemple g1) dans le champ aller à l'interface et cliquez sur le bouton aller.**
 - Pour configurer plusieurs interfaces avec les mêmes paramètres, cochez la case associée à chaque interface.
 - Pour configurer toutes les interfaces avec les mêmes paramètres, cochez la case dans la ligne d'en-tête.
8. Dans le menu **IPv6SG mode**, spécifiez le mode d'administration d'IPv6SG sur l'interface :
- Activer. IPv6SG est activé sur l'interface. L'adresse IPv6 de la source n'est pas dans la base de données de liaison DHCP Snooping, les paquets ne sont pas transférés.
 - Désactiver : IPv6SG est désactivé sur l'interface. La valeur par défaut est désactiver.
9. Dans le menu **sécurité du port IPv6SG**, spécifiez le mode d'administration de la sécurité du port IPv6SG sur l'interface :
- Activer. La sécurité du port IPv6SG est activée sur l'interface. Les paquets ne sont pas transférés si l'adresse MAC de la source ne se trouve pas dans la table de la base de données de transfert ou dans la base de données de liaison de surveillance DHCP. Pour appliquer le filtrage basé sur l'adresse MAC, vous devez également configurer les fonctionnalités suivantes :
 - Activez la sécurité des ports globalement (voir [Configurez le mode de sécurité du port global](#) à la page 919).
 - Activez la sécurité des ports sur l'interface (voir [Configurer une interface de sécurité de port](#) à la page 920).
 - Désactiver : La sécurité du port IPv6SG est désactivée sur l'interface. La valeur par défaut est désactiver.
10. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

11. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Ajoutez une liaison de protection source IPv6 statique et affichez ou effacez les liaisons de protection source IPv6 dynamiques

Vous pouvez ajouter une liaison statique dans la base de données de liaisons IPv6 source Guard (IPv6SG) et afficher ou effacer les liaisons dynamiques dans la table de liaisons.

Pour ajouter une liaison IPv6SG statique et afficher ou effacer les liaisons IPv6SG dynamiques :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > contrôle > IPv6 source Guard > Configuration de liaison**.

La page Configuration de la liaison s'affiche.

6. Dans le menu **interface**, sélectionnez l'interface.
7. Dans le champ **adresse MAC**, spécifiez l'adresse MAC de la liaison à ajouter.
C'est la clé de la base de données de liaison.
8. Dans le menu **VLAN ID**, sélectionnez l'ID du VLAN.
9. Dans le champ **adresse IPv6**, spécifiez l'adresse IPv6 pour la liaison à ajouter.
10. Cliquez sur le bouton **Add** (Ajouter).

L'entrée de liaison statique IPv6SG est ajoutée à la base de données.

Le champ type de filtre s'affiche si IPv6SG est configuré pour fonctionner avec l'adresse IPv6 source uniquement ou, si la sécurité du port est également activée pour IPv6SG, avec l'adresse IPv6 source et l'adresse MAC.

Le tableau Configuration de la liaison dynamique affiche des informations sur les liaisons IPv6SG apprises sur chaque interface sur laquelle IPv6SG est activé. Le tableau suivant décrit les informations de liaison dynamique.

Champ	Description
Interface	Interface sur laquelle la liaison source IPv6SG a été apprise.
Adresse MAC	Adresse MAC associée au périphérique source IPv6SG. C'est la clé de la base de données de liaison.
Identifiant VLAN	ID VLAN de l'interface du périphérique source IPv6SG.
Adresse IPv6	Adresse IPv6 du périphérique source IPv6SG.
Type de filtre	Type de filtre utilisé sur l'interface du commutateur. IPv6SG est configuré pour fonctionner avec l'adresse IPv6 source uniquement ou, si la sécurité du port est également activée pour IPv6SG, avec l'adresse IPv6 source et l'adresse MAC.

11. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.
12. Pour effacer toutes les liaisons dynamiques du tableau Configuration de liaison dynamique, cliquez sur le bouton **Effacer**.
13. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimez une liaison statique IPv6 source Guard

Vous pouvez supprimer une liaison statique de la base de données de liaisons IPv6 source Guard (IPv6SG).

Pour supprimer une liaison IPv6SG statique :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > contrôle > IPv6 source Guard > Configuration de liaison**.

La page Configuration de la liaison s'affiche.

6. Dans le tableau Configuration de la liaison statique, cochez la case de la liaison statique.
7. Cliquez sur le bouton **Supprimer**.

L'entrée de liaison IPv6SG est supprimée de la base de données.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Inspection ARP dynamique

L'inspection ARP dynamique (DAI) est une fonction de sécurité qui rejette les paquets ARP non valides et malveillants. Empêche les attaques de type man-in-the-middle, où une station malveillante intercepte le trafic d'autres stations en empoisonnant les caches ARP des postes voisins. La station hostile envoie des requêtes ARP ou des réponses mappant l'adresse IP d'une autre station à sa propre adresse MAC.

DAI s'appuie sur DHCP Snooping. DHCP Snooping écoute les échanges de messages DHCP et construit une base de données de liaisons des adresses MAC valides, des adresses IP, des interfaces VLAN, etc.

Si DAI est activé et si l'adresse MAC de l'expéditeur et l'adresse IP de l'expéditeur ne correspondent pas à une entrée dans la base de données DHCP Snooping bindings, le commutateur supprime le paquet ARP IF. Cependant, vous pouvez également créer des mappages statiques dans la base de données de liaisons DHCP Snooping. Les mappages statiques sont utiles lorsque les hôtes configurent des adresses IP statiques, que le commutateur ne peut pas exécuter la surveillance DHCP ou que d'autres commutateurs du réseau n'exécutent pas d'inspection ARP dynamique. Un mappage statique associe une adresse IP à une adresse MAC sur un VLAN.

Vous pouvez configurer des VLAN DAI, des interfaces et des listes de contrôle d'accès (ACL) avec des règles associées.

Configurez les paramètres DAI globaux

Vous pouvez configurer les paramètres DAI (Global Dynamic ARP inspection).

Pour configurer les paramètres DAI globaux :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.
4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.
5. Sélectionnez **sécurité > contrôle > inspection ARP dynamique > Configuration DAI** .

L'écran DAI Configuration (Configuration IP) s'affiche.
6. Sélectionnez le bouton radio valider la **désactivation** ou **l'activation de** l'adresse MAC source.

Ce paramètre spécifie le mode de validation MAC source DAI pour le commutateur. Si vous sélectionnez Activer, l'adresse MAC de l'expéditeur dans un paquet ARP est validée. La valeur par défaut est désactiver.
7. Sélectionnez le bouton radio valider la **désactivation** MAC de destination ou **Activer**

Ce paramètre spécifie le mode de validation MAC de destination DAI pour le commutateur. Si vous sélectionnez Activer, l'adresse MAC de destination dans un paquet de réponse ARP est validée. La valeur par défaut est désactiver.
8. Sélectionnez le bouton radio valider IP **désactiver** ou **Activer**.

Ce paramètre spécifie le mode de validation IP DAI pour le commutateur. Si vous sélectionnez Activer, l'adresse IP d'un paquet ARP est validée. La valeur par défaut est désactiver.
9. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.
10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurer les VLAN DAI

Vous pouvez configurer un ou plusieurs VLAN d'inspection ARP dynamique (DAI).

Pour configurer un ou plusieurs VLAN DAI :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > contrôle > inspection ARP dynamique > Configuration DAI VLAN**.

La page de configuration DAI VLAN s'affiche.

Le tableau répertorie les VLAN.

6. Cochez les cases correspondant au contenu.

7. Dans le menu **mode Admin**, sélectionnez **Activer** ou **désactiver** pour spécifier si DAI est activé pour le VLAN.

La valeur par défaut est désactiver.

8. Dans le menu **paquets non valides**, sélectionnez **Activer** ou **désactiver** pour spécifier si la journalisation DAI est activée pour le VLAN.

La valeur par défaut est Activer.

9. Dans le champ **nom de la liste de contrôle d'accès ARP**, spécifiez le nom d'une liste de contrôle d'accès ARP existante (voir [Créez une liste de contrôle d'accès DAI](#) à la page 1002).

L'ACL ARP est utilisée pour la validation des paquets ARP. Pour supprimer un nom de liste de contrôle d'accès ARP existant du champ **nom de liste de contrôle d'accès ARP**, entrez **N/A**.

10. Dans le menu **Static Flag**, sélectionnez **Enable** ou **Disable** pour spécifier si le paquet ARP doit être validé à l'aide de la base de données DHCP Snooping si la règle ARP ACL ne correspond pas.

Si cette option est activée, le paquet ARP est validé uniquement par la règle ARP ACL. Si cette option est désactivée, le paquet ARP doit être validé à l'aide de la base de données DHCP Snooping. La valeur par défaut est désactiver.

11. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

12. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurer les interfaces DAI

Vous pouvez configurer une ou plusieurs interfaces DAI (Dynamic ARP inspection).

Pour configurer une ou plusieurs interfaces DAI :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > contrôle > inspection ARP dynamique > Configuration de l'interface DAI**.

La page Configuration de l'interface DAI s'affiche.

6. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :

- **1 ou ID d'unité pour un commutateur empilé :**
 - 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
 - **ID d'unité pour un commutateur empilé :** Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
- **LAG** Seuls les LAG sont affichés.
- **Tous:** Les interfaces physiques et les LAG sont affichés, ou pour une pile de commutateurs, les interfaces physiques de tous les commutateurs de la pile et les LAG sont affichés.

7. Sélectionnez une ou plusieurs interfaces en effectuant l'une des actions suivantes :

- **Pour configurer une interface unique, cochez la case associée au port ou tapez le numéro de port (par exemple g1) dans le champ aller à l'interface et cliquez sur le bouton aller.**
- Pour configurer plusieurs interfaces avec les mêmes paramètres, cochez la case associée à chaque interface.
- Pour configurer toutes les interfaces avec les mêmes paramètres, cochez la case dans la ligne d'en-tête.

8. Dans le menu **Trust mode**, spécifiez si l'interface est approuvée pour DAI.

Si cette option est activée, l'interface est approuvée et les paquets ARP entrant dans l'interface sont transférés sans vérification. Si cette option est désactivée, l'interface n'est pas approuvée et les paquets ARP entrant dans l'interface sont soumis à DAI. La valeur par défaut est désactiver.

9. Dans le champ **Rate Limit (PPS)**, spécifiez la valeur de la limite de débit pour DAI. Si le débit entrant des paquets ARP dépasse la valeur spécifiée pendant des secondes d'intervalle de rafale consécutives, les paquets ARP sont abandonnés. Si vous spécifiez N/A, aucune limite n'existe. La plage est de 0 à 300. La valeur par défaut est de 15 paquets par seconde (PPS).
10. Dans le champ **intervalle de rafale (sec)**, spécifiez la valeur de l'intervalle de rafale pour la limitation de débit sur l'interface. Si vous spécifiez N/A, l'intervalle de rafale n'est pas effectif. La plage est de 1 à 15. La valeur par défaut est 1 seconde.
11. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
12. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Créez une liste de contrôle d'accès DAI

Vous pouvez créer une liste de contrôle d'accès (ACL) d'inspection ARP dynamique (DAI) à laquelle vous pouvez ensuite ajouter des règles.

Pour créer une ACL DAI :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > contrôle > inspection ARP dynamique > Configuration DAI ACL**.

La page Configuration de la liste de contrôle d'accès DAI s'affiche.

6. Dans le champ Nom, entrez un nom de 31 caractères maximum.

7. Cliquez sur le bouton **Add** (Ajouter).

L'ACL DAI est ajoutée.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez une règle pour une ACL DAI existante

Après avoir ajouté une ACL DAI (voir [Créez une liste de contrôle d'accès DAI](#) à la page 1002), vous pouvez configurer une règle pour informatique.

Pour configurer une règle pour une ACL DAI existante :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **sécurité > contrôle > inspection ARP dynamique > Configuration des règles ACL DAI**.
La page Configuration de la règle ACL DAI s'affiche.
6. Dans le menu **nom de la liste de contrôle d'accès**, sélectionnez la liste de contrôle d'accès DAI pour laquelle vous souhaitez configurer la règle.
7. Dans le menu **action**, sélectionnez l'action qui doit se produire si un paquet correspond aux critères de la règle :
 - **Permis** : Le paquet est autorisé et transmis.
 - **Refuser** : Le paquet est refusé et abandonné.
8. Dans le champ **adresse IP source**, entrez l'adresse IP source qui doit être utilisée comme correspondance pour la règle.
9. Dans le champ **adresse MAC source**, entrez l'adresse MAC source qui doit être utilisée comme correspondance pour la règle.
10. Cliquez sur le bouton **Add** (Ajouter).
La règle est ajoutée.
11. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimer une règle d'une liste de contrôle d'accès DAI existante

Vous pouvez supprimer une règle d'une liste de contrôle d'accès DAI existante.

Pour supprimer une règle d'une liste de contrôle d'accès DAI existante :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > contrôle > inspection ARP dynamique > Configuration des règles ACL DAI**.

La page Configuration de la règle ACL DAI s'affiche.

6. Dans le menu **nom de la liste de contrôle d'accès**, sélectionnez la liste de contrôle d'accès DAI dont vous souhaitez supprimer une règle.

7. Cochez la case de la règle.

8. Cliquez sur le bouton **Supprimer**.

La règle est supprimée.

9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimer une liste de contrôle d'accès DAI

Vous pouvez supprimer une liste de contrôle d'accès (ACL) DAI (inspection ARP dynamique) dont vous n'avez plus besoin.

Pour supprimer une ACL DAI :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > contrôle > inspection ARP dynamique > Configuration DAI ACL**.

La page Configuration de la liste de contrôle d'accès DAI s'affiche.

6. Cochez les cases correspondant au contenu.

7. Cliquez sur le bouton **Supprimer**.

L'ACL DAI est supprimée.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Afficher les statistiques DAI

Pour afficher les statistiques DAI :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > contrôle > inspection ARP dynamique > statistiques DAI**.

La page DAI Statistic s'affiche.

6. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

7. Pour effacer les statistiques, cliquez sur le bouton **Effacer**.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 178 : Informations statistiques DAI

Champ	Description
VLAN	L'identifiant VLAN.
DROPs DHCP	Nombre de paquets ARP abandonnés par DAI car aucune entrée de liaison DHCP correspondante n'existe.
Autorisations DHCP	Nombre de paquets ARP qui ont été transférés par DAI parce qu'une entrée de liaison DHCP correspondante existe.
DROPs ACL	Nombre de paquets ARP abandonnés par DAI parce qu'il n'existe aucune règle ACL ARP correspondante pour le VLAN et que l'indicateur statique est défini sur le VLAN.
Autorisations ACL	Nombre de paquets ARP autorisés par DAI car une règle ACL ARP correspondante existe pour le VLAN.
Adresse MAC source incorrecte	Nombre de paquets ARP abandonnés par DAI parce que l'adresse MAC de l'expéditeur dans les paquets ARP ne correspond pas à l'adresse MAC source dans l'en-tête Ethernet.
Adresse MAC incorrecte	Nombre de paquets ARP abandonnés par DAI parce que l'adresse MAC cible dans les paquets de réponse ARP ne correspond pas à l'adresse MAC de destination dans l'en-tête Ethernet.
IP non valide	Nombre de paquets ARP abandonnés par DAI parce que l'adresse IP de l'expéditeur dans les paquets ARP ou l'adresse IP cible dans les paquets de réponse ARP n'est pas valide. Les adresses non valides incluent 0,0,0,0, 255.255.255.255, les adresses IP multicast, les adresses de classe E (240.0,0,0/4) et les adresses de bouclage (127.0,0,0/8).
Suivant	Nombre de paquets ARP valides transmis par DAI.
Abandonné	Nombre de paquets ARP non valides abandonnés par DAI.

Portail captif

La fonction de portail captif vous permet d'empêcher les clients d'accéder au réseau jusqu'à ce que la vérification de l'utilisateur soit établie. Vous pouvez configurer la vérification du portail captif pour autoriser l'accès aux utilisateurs invités et authentifiés. Les utilisateurs authentifiés doivent être validés par rapport à une base de données d'utilisateurs de portail captif autorisés avant que l'accès ne soit accordé. La base de données peut être stockée localement sur le commutateur ou sur un serveur RADIUS.

Le serveur d'authentification prend en charge les connexions Web HTTP et HTTPS. En outre, vous pouvez configurer un portail captif pour utiliser un port HTTP facultatif (pour la prise en charge des réseaux proxy HTTP). S'il est configuré, ce port supplémentaire est alors utilisé exclusivement par le portail captif. Ce port facultatif s'ajoute au port HTTP standard 80, qui est utilisé pour tout autre trafic Web.

Si vous activez la fonctionnalité de portail captif sur un port, le port supprime tout le trafic des clients non authentifiés, à l'exception des paquets ARP, DHCP, DNS et

NETBIOS, qui sont transférés pour que les clients non authentifiés puissent obtenir une adresse IP et résoudre le nom d'hôte ou les noms de domaine. Le trafic de données des clients authentifiés passe par, et les règles ne s'appliquent pas à ces paquets.

Pour un port sur lequel vous activez la fonctionnalité de portail captif, si un client non authentifié ouvre un navigateur Web et tente de se connecter au réseau, le portail captif redirige tout le trafic HTTP et HTTPS des clients non authentifiés vers le serveur d'authentification sur le commutateur. Une page Web de portail captif s'affiche pour le client non authentifié, permettant au client de s'authentifier, après quoi le client reçoit l'accès au port.

La fonctionnalité de portail captif n'est pas prise en charge pour les interfaces VLAN, les interfaces de bouclage et les interfaces logiques. La fonctionnalité de portail captif utilise l'authentification basée sur l'adresse MAC et non l'authentification basée sur le port. Cela signifie que tous les clients connectés à l'interface du portail captif doivent être authentifiés avant de pouvoir accéder au réseau.

Configurez les paramètres globaux du portail captif

Vous pouvez contrôler l'état administratif de la fonctionnalité de portail captif et configurer les paramètres globaux qui affectent tous les portails captifs que vous configurez sur le commutateur.

Pour configurer les paramètres globaux du portail captif :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > contrôle > Portail captif > Configuration globale CP**.

La page Configuration globale CP s'affiche.

6. Sélectionnez le bouton radio désactiver ou Activer le mode EEE.

Cette sélection définit le mode administratif de la fonctionnalité de portail captif. La valeur par défaut est désactiver.

7. Dans le champ **Port HTTP supplémentaire**, entrez un numéro de port compris entre 0 et 65535, à l'exception du port 80.

Le trafic HTTP utilise le port standard 80, mais vous pouvez configurer un port supplémentaire pour le trafic HTTP. La valeur par défaut est 0, ce qui désactive cette option.

8. Dans le champ **Additional HTTP Secure Port**, entrez un numéro de port compris entre 0 et 65535, à l'exception du port 443.

Le trafic HTTP Secure (HTTPS) utilise le port standard 443, mais vous pouvez configurer un port supplémentaire pour le trafic HTTPS. La valeur par défaut est 0, ce qui désactive cette option.

9. Dans le champ **délai d'authentification**, entrez le nombre de secondes pendant lesquelles une session d'authentification reste ouverte pendant qu'un client tente d'accéder au réseau via un portail captif.

Pour accéder au réseau via un portail captif, le client doit d'abord saisir les informations d'authentification sur une page Web d'authentification. Lorsque le délai d'expiration de la session d'authentification expire et que le client n'est pas encore authentifié, le commutateur déconnecte toute connexion TCP ou SSL active avec le client. La plage est de 60 à 600 secondes. La valeur par défaut est de 300 secondes.

10. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

11. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 179 : Informations de configuration globale du portail captif

Champ	Description
Statut opérationnel	État opérationnel de la fonctionnalité de portail captif, qui est activé ou Désactivé.
Motif désactivé	Si la fonctionnalité de portail captif est désactivée, la raison pour laquelle informatique est désactivé : • Administrateur désactivé • Adresse IP non configurée • Aucune interface de routage IP • Routage désactivé
Adresse IP CP	Adresse IP utilisée par le portail captif.
Portails captifs pris en charge	Nombre total de portails captifs pris en charge sur le commutateur.
Portails captifs configurés	Nombre de portails captifs configurés sur le commutateur.
Portails captifs actifs	Nombre de portails captifs activés (actifs).
Utilisateurs pris en charge par le système	Nombre total d'utilisateurs pouvant être authentifiés localement et à distance sur le commutateur.
Utilisateurs locaux pris en charge	Nombre total d'utilisateurs pouvant être authentifiés localement sur le commutateur.
Utilisateurs locaux configurés	Nombre d'utilisateurs locaux configurés sur le commutateur.
Utilisateurs authentifiés	Nombre d'utilisateurs authentifiés pour tous les portails captifs du commutateur.

Configurer un portail captif

Par défaut, le commutateur fournit un portail captif par défaut. Vous pouvez modifier les paramètres du portail captif par défaut. Vous pouvez également ajouter et configurer jusqu'à neuf portails supplémentaires.

Pour configurer une instance de portail captif :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > contrôle > Portail captif > Configuration CP**.

L'écran CP Configuration (Configuration IP) s'affiche.

6. Pour effectuer l'une des opérations suivantes :

- **Modifier le portail captif par défaut** : En regard du champ **ID CP**, cochez la case **1**.
- **Ajouter un nouveau portail captif** : Dans le menu **CP ID**, sélectionnez un ID compris entre **2** et **10**.
- **Modifier un portail captif que vous avez ajouté avant** : En regard du champ **ID CP**, cochez la case associée au portail captif.

7. Dans le champ **nom CP**, spécifiez un nom pour le portail captif.

Le nom peut comporter jusqu'à 31 caractères.

8. Dans le menu du mode EEE, sélectionnez Activer ou désactiver.

Cette sélection définit le mode administratif du portail captif. Par défaut, un portail captif est désactivé.

9. Dans le champ **Protocole**, sélectionnez **HTTP** ou **HTTPS** utilisé pour la communication avec les clients pendant le processus de vérification :

- HTTP : N'utilise pas le cryptage pendant la vérification.
 - HTTPS Utilise le protocole SSL (Secure Sockets Layer), qui nécessite un certificat pour le cryptage. Le certificat est présenté à l'utilisateur au moment de la connexion.
10. Dans le menu **vérification**, sélectionnez le type d'authentification utilisateur que le portail captif utilise lorsqu'un client tente de se connecter :
- Invités : Aucune authentification utilisateur n'est requise.
 - Local L'utilisateur est authentifié via la base de données locale.
 - RADIUS L'utilisateur est authentifié via un serveur RADIUS.
11. Sélectionnez l'état de blocage, qui permet de contrôler rapidement et temporairement un portail captif lors d'événements inattendus, tels que des attaques par déni de service :
- Désactiver : La fonction de blocage est désactivée. Vous ne pouvez pas bloquer rapidement le portail captif.
 - Activer. Le portail captif est bloqué.
 - **Non bloqué** : Le portail captif n'est pas bloqué. La valeur par défaut n'est pas bloquée.
12. Dans le menu **Groupe**, sélectionnez un groupe d'utilisateurs de portail captif existant pour le portail captif.
- Tous les utilisateurs appartenant au groupe sont autorisés à accéder au réseau via le portail captif.
- Cette option est disponible uniquement si vous sélectionnez **local** ou **RADIUS** dans le menu **vérification**.
13. Dans le champ **délai d'inactivité**, entrez le nombre de secondes pendant lesquelles le commutateur attend avant de mettre fin à une session inactive et de déconnecter l'utilisateur.
- La plage est de 0 à 900 secondes. La valeur par défaut est 0 seconde, ce qui signifie que le délai d'attente n'est pas appliqué.
14. Dans le menu **déconnexion de l'utilisateur**, spécifiez si un client authentifié peut se déconnecter du portail captif et du réseau :
- Activer. Un utilisateur peut délibérément se déconnecter du portail captif et du réseau.
 - Désactiver : Un utilisateur ne peut pas se déconnecter du portail captif et du réseau, ce qui fait que l'état de la connexion reste authentifié jusqu'à ce que le portail captif désauthentifie l'utilisateur, par exemple parce que le délai d'inactivité ou le délai d'expiration de session est dépassé.

15. Si le mode de vérification est RADIUS (c'est-à-dire que vous sélectionnez **RADIUS** dans le menu **vérification**), spécifiez l'adresse IP du serveur RADIUS dans le champ **serveur d'authentification Radius**.
16. Dans le menu **mode redirection**, spécifiez si les clients nouvellement authentifiés sont redirigés vers une URL :
 - Activer. Les clients authentifiés sont redirigés vers une URL que vous pouvez spécifier dans le champ URL de redirection.
 - Désactiver : Les clients authentifiés ne sont pas redirigés et le paramètre régional par défaut « Welcome » est utilisé. La valeur par défaut est désactiver.
17. Dans le champ **URL de redirection**, spécifiez l'URL vers laquelle les clients nouvellement authentifiés doivent être redirigés.

La longueur maximale de l'URL est de 512 caractères alphanumériques. L'URL par défaut est `http:// <ipaddress> /v1/Security/captive_Portal/cp_welcome.html`.

Cette option est disponible uniquement si vous sélectionnez **Activer** dans le menu **mode redirection**.
18. Dans le champ **couleur d'arrière-plan**, spécifiez la valeur de la couleur d'arrière-plan.

La couleur par défaut est #BFBFBF.
19. Dans le champ **couleur de premier plan**, spécifiez la valeur de la couleur de premier plan.

La couleur par défaut est #999999.
20. Dans le champ **couleur du séparateur**, spécifiez la valeur de la couleur du séparateur.

La couleur par défaut est #B70024.
21. Dans le champ **Max Bandwidth Down**, spécifiez le débit maximal auquel un client peut recevoir des données du réseau.

Le débit est exprimé en octets par seconde. La plage est de 0 à 536870911. La valeur par défaut est 0, ce qui indique que la limite n'est pas appliquée.
22. Dans le champ **Max Bandwidth Up**, spécifiez le débit maximal auquel un client peut envoyer des données sur le réseau.

Le débit est exprimé en octets par seconde. La plage est de 0 à 536870911. La valeur par défaut est 0, ce qui indique que la limite n'est pas appliquée.
23. Dans le champ **entrée max**, spécifiez le nombre maximal d'octets qu'un client est autorisé à recevoir.

Une fois cette limite atteinte, le client est déconnecté. La plage est de 0 à 4294967295. La valeur par défaut est 0, ce qui indique que la limite n'est pas appliquée.
24. Dans le champ **Max Output**, spécifiez le nombre maximal d'octets qu'un client est autorisé à transmettre.

Une fois cette limite atteinte, le client est déconnecté. La plage est de 0 à 4294967295. La valeur par défaut est 0, ce qui indique que la limite n'est pas appliquée.

25. Dans le champ **total max**, spécifiez le nombre maximal d'octets qu'un client est autorisé à transférer, c'est-à-dire la somme des octets transmis et reçus.

Une fois cette limite atteinte, le client est déconnecté. La plage est de 0 à 4294967295. La valeur par défaut est 0, ce qui indique que la limite n'est pas appliquée.

26. Effectuez l'une des opérations suivantes :

- Si vous ajoutez un nouveau portail captif, cliquez sur le bouton **Ajouter**.
Les paramètres sont enregistrés. Le portail captif est ajouté.
- Si vous modifiez le portail captif par défaut ou un portail captif que vous avez ajouté auparavant, cliquez sur le bouton **appliquer**.
Les paramètres sont enregistrés.

27. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimer un portail captif

Vous pouvez supprimer un portail captif dont vous n'avez plus besoin.

Pour supprimer un portail captif :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > contrôle > Portail captif > Configuration CP**.

L'écran CP Configuration (Configuration IP) s'affiche.

6. Cochez la case du portail captif.

7. Cliquez sur le bouton **Supprimer**.

Le portail captif est supprimé.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurer une liaison de portail captif

Vous pouvez associer un portail captif à une ou plusieurs interfaces. Bien que vous puissiez associer plusieurs interfaces à un seul portail captif, vous ne pouvez associer une interface qu'à un seul portail captif.

Pour configurer une liaison de portail captif :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > contrôle > Portail captif > Configuration de liaison CP**.

La page Configuration de liaison CP s'affiche.

6. Dans le menu **CP ID**, sélectionnez le portail captif.

Le champ nom CP affiche le nom du portail captif.

7. Pour ajouter le portail captif sélectionné à un port, dans la table ports (ou, si une pile est configurée, dans l'une des tables ports), cliquez sur le port pour qu'une coche s'affiche.

Vous pouvez ajouter le portail captif à plusieurs ports.

Les ports du commutateur (unité 1) sont affichés. Si une pile est configurée, les ports de chaque commutateur empilé (unité 1, unité 2, etc.) sont affichés et vous pouvez sélectionner des ports sur différents commutateurs empilés.

8. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Afficher ou supprimer des liaisons de portail captif dans la table de liaison de portail captif

Vous pouvez afficher ou supprimer des liaisons pour les portails captifs.

Pour afficher ou supprimer des liaisons de portail captif :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > contrôle > Portail captif > table de liaison CP**.

La page table de liaison CP s'affiche. Ce tableau affiche les liaisons captives portail-interface.

6. Pour supprimer une liaison captive portail-interface, procédez comme suit :
 - a. Cochez la case en regard de l'interface.
 - b. Cliquez sur le bouton **Supprimer**.

La liaison est supprimée.

7. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

8. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

Le tableau suivant décrit les champs en lecture seule de la page.

Table 180 : Informations de liaison de portail captif

Champ	Description
Interface	Interface à laquelle le portail captif est lié.
ID CP	ID du portail captif.
Statut opérationnel	Indique si le portail est actif sur l'interface (désactiver ou Activer).
État du bloc	Indique si le portail captif est temporairement bloqué pour authentification.
Utilisateurs authentifiés	Nombre d'utilisateurs authentifiés via le portail captif sur l'interface.

Configurer des groupes de portails captifs

Les groupes de portail captif vous permettent d'organiser les utilisateurs du portail captif, ce qui est utile si un grand nombre d'utilisateurs doivent pouvoir accéder à un portail captif. Après avoir ajouté un groupe de portails captifs, vous pouvez ajouter des utilisateurs au groupe.

Par défaut, tous les utilisateurs du portail captif sont ajoutés au groupe par défaut avec l'ID 1. Vous pouvez ajouter jusqu'à 10 groupes.

Ajouter un groupe de portails captifs

Après avoir ajouté un groupe de portail captif, vous pouvez ajouter des utilisateurs de portail captif au groupe (voir [Configurer les utilisateurs du portail captif](#) à la page 1021).

Pour ajouter un groupe de portails captifs :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > contrôle > Portail captif > Configuration du groupe CP**

La page Configuration du groupe CP s'affiche.

6. Dans le menu **ID de groupe**, sélectionnez un ID pour le groupe.

Vous pouvez sélectionner un ID compris entre **1** et **10**.

7. Dans le champ **nom du groupe**, spécifiez un nom pour le groupe.

Le nom peut contenir de 1 à 31 caractères alphanumériques.

8. Cliquez sur le bouton **Add** (Ajouter).

Le groupe est ajouté.

9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimer un groupe de portails captifs

Vous pouvez supprimer un groupe de portails captifs dont vous n'avez plus besoin.

Pour supprimer un groupe de portails captifs :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **sécurité > contrôle > Portail captif > Configuration du groupe CP**.
La page Configuration du groupe CP s'affiche.
6. Dans le menu **ID de groupe**, sélectionnez un ID pour le groupe.
Vous pouvez sélectionner un ID compris entre **1** et **10**.
7. Cochez la case correspondant au groupe à supprimer.
8. Cliquez sur le bouton **Supprimer**.
Le groupe est supprimé.
9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurer les utilisateurs du portail captif

Vous pouvez configurer les paramètres des utilisateurs de portail captif et les ajouter à un groupe de portail captif. Par défaut, tous les utilisateurs captifs sont ajoutés au groupe par défaut avec l'ID 1. Après avoir ajouté un groupe de portail captif personnalisé (voir [Configurer des groupes de portails captifs](#) à la page 1019), vous pouvez également affecter des utilisateurs de portail captif au groupe personnalisé.

Les paramètres que vous pouvez configurer pour un utilisateur de portail captif individuel incluent un mot de passe, des périodes de temporisation, des largeurs de bande et des volumes de trafic maximum.

Ajouter ou modifier un compte utilisateur de portail captif

Vous pouvez ajouter un compte utilisateur de portail captif ou modifier un compte existant.

Pour ajouter ou modifier un compte utilisateur de portail captif :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > contrôle > Portail captif > Configuration utilisateur CP**.

La page Configuration utilisateur CP s'affiche.

6. Si vous modifiez les paramètres d'un compte d'utilisateur existant, cochez la case correspondant au compte d'utilisateur.

Si vous modifiez les paramètres, vous ne pouvez pas modifier l'ID utilisateur et le nom d'utilisateur.

7. Si vous ajoutez un compte utilisateur, dans le champ **ID utilisateur**, spécifiez un ID compris entre **1** et **99** pour identifier l'utilisateur.

Après avoir ajouté le compte utilisateur, vous ne pouvez pas modifier l'ID.

8. Si vous ajoutez un compte d'utilisateur, dans le champ **nom d'utilisateur**, entrez un nom pour le compte d'utilisateur.

Le nom du tunnel peut contenir jusqu'à 31 caractères alphanumériques. Après avoir ajouté le compte utilisateur, vous ne pouvez pas modifier le nom.

9. Dans le menu **modifier le mot de passe**, sélectionnez pour utiliser un mot de passe ou aucun mot de passe pour le nouveau compte utilisateur :
- Activer. Les champs mot de passe et confirmer le mot de passe ne sont pas masqués afin que vous puissiez spécifier un mot de passe unique pour le nouveau compte utilisateur :
 - Dans le champ **mot de passe**, spécifiez un mot de passe de 8 à 64 caractères.
 - Dans le champ **confirmer le mot de** passe, spécifiez à nouveau le mot de passe.
 - Désactiver : Les champs mot de passe et confirmer le mot de passe sont masqués et vous ne pouvez pas spécifier de mot de passe pour le nouveau compte utilisateur.

Par défaut, la sélection est désactiver, ce qui signifie qu'aucun mot de passe n'est utilisé et que les champs de mot de passe sont masqués.

10. Dans le menu **Groupe**, sélectionnez au moins un groupe de portails captifs.

Pour attribuer un compte utilisateur à plusieurs groupes, appuyez sur la touche **Ctrl de** votre clavier et sélectionnez chaque groupe. Par défaut, un nouveau compte utilisateur est attribué au groupe par défaut avec l'ID 1.

11. Dans le champ **délai de session**, entrez la période en secondes pendant laquelle un utilisateur est autorisé à rester connecté au réseau.

Une fois le délai d'expiration de la session dépassé, l'utilisateur est automatiquement déconnecté. La valeur par défaut est 0, ce qui signifie que la session n'expire pas. La plage est de 0 à 86400 secondes.

12. Dans le champ **délai d'inactivité**, entrez la durée en secondes pendant laquelle le commutateur attend avant de mettre fin à une session inactive et de déconnecter l'utilisateur.

La valeur par défaut est 0, ce qui signifie qu'une session inactive n'expire pas. La plage est de 0 à 900 secondes.

13. Dans le champ **Max Bandwidth Down**, entrez le débit maximal, en bits par seconde, auquel un client peut recevoir des données du réseau.

Une valeur de 0 indique que la configuration globale doit être utilisée. La plage est de 0 à 536870911 secondes.

14. Dans le champ **Max Bandwidth Up**, entrez le débit maximal, en bits par seconde, auquel un client peut envoyer des données sur le réseau.

Une valeur de 0 indique que la configuration globale doit être utilisée. La plage est de 0 à 536870911 secondes.

15. Dans le champ **entrée max.**, entrez le nombre d'octets que l'utilisateur est autorisé à recevoir.

Une fois cette limite atteinte, l'utilisateur est déconnecté. Une valeur de 0 indique que la limite globale doit être utilisée. La plage est de 0 à 4294967295.

16. Dans le champ **Max Output**, entrez le nombre d'octets que l'utilisateur est autorisé à transmettre.

Une fois cette limite atteinte, l'utilisateur est déconnecté. Une valeur de 0 indique que la limite globale doit être utilisée. La plage est de 0 à 4294967295.

17. Dans le champ **total max.**, entrez le nombre d'octets que l'utilisateur est autorisé à transmettre et à recevoir.

Le nombre maximal d'octets correspond à la somme des octets transmis et reçus. Une fois cette limite atteinte, l'utilisateur est déconnecté. Une valeur de 0 indique que la limite globale doit être utilisée. La plage est de 0 à 4294967295.

18. Effectuez l'une des opérations suivantes :

- Si vous ajoutez un nouveau compte utilisateur, cliquez sur le bouton **Ajouter**.
Les paramètres sont enregistrés. Le compte utilisateur est ajouté.
- Si vous modifiez les paramètres d'un compte utilisateur, cliquez sur le bouton **appliquer**.
Les paramètres sont enregistrés.

19. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimer un compte utilisateur de portail captif

Vous pouvez supprimer un compte utilisateur de portail captif qui n'est plus nécessaire.

Pour supprimer un compte utilisateur de portail captif :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > contrôle > Portail captif > Configuration utilisateur CP**.

La page Configuration utilisateur CP s'affiche.

6. Cochez la case correspondant au compte utilisateur.

7. Cliquez sur le bouton **Supprimer**.

Le compte utilisateur est supprimé.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez les paramètres des indicateurs de trappe de portail captif

Vous pouvez spécifier si le commutateur envoie des interruptions SNMP pour les actions qui se produisent sur le portail captif. Par défaut, le commutateur n'envoie pas de traps pour les actions qui se produisent sur le portail captif.

Pour configurer les paramètres des indicateurs de trappe de portail captif :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > contrôle > Portail captif > drapeaux d'interruption CP** .

La page drapeaux de trappe CP s'affiche.

6. Configurez les paramètres d'indicateur d'interruption suivants :

- **Mode Trap CP** : Activer ou désactiver le mode de trappe captive.
- **Échec de l'authentification du client** : Activer ou désactiver la transmission d'une interruption si un client ne parvient pas à s'authentifier auprès d'un portail captif.
- **client connecté** Activer ou désactiver la transmission d'une interruption si un client s'authentifie auprès d'un portail captif et s'y connecte.
- **Base de données client complète** : Activez ou désactivez la transmission d'une interruption chaque fois qu'une entrée ne peut pas être ajoutée à la base de données client car informatique est saturé.
- **Déconnexion du client** : Activer ou désactiver la transmission d'une interruption si un client se déconnecte d'un portail captif.

Par défaut, ces paramètres d'indicateur de déroutement sont désactivés.

7. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Afficher ou effacer les statistiques des clients du portail captif

Vous pouvez afficher ou effacer les statistiques des clients du portail captif, y compris les statistiques sur le trafic envoyé et reçu par des clients individuels.

Pour afficher ou effacer les statistiques client du portail captif :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > contrôle > Portail captif > Client CP**.

La page CP Client s'affiche.

6. Pour rechercher un utilisateur de portail captif par adresse MAC, spécifiez l'adresse MAC, puis cliquez sur le bouton **aller**.

Si l'entrée existe, les informations relatives à l'utilisateur du portail captif s'affichent. Une correspondance exacte est requise.

7. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

8. Pour effacer les statistiques client du portail captif, cliquez sur le bouton **Effacer**.
9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 181 : Statistiques des clients du portail captif

Champ	Description
Adresse MAC	Adresse MAC du client.
DROPs d'adresse IP	Adresse IP du client
Protocole	Le protocole de connexion, qui est HTTP ou HTTPS.
Vérification	Le type d'authentification, qui est invité, local ou RADIUS.
Durée de la session	Période écoulée depuis que le client a été autorisé.
Interface	Interface utilisée par le client.
ID CP	ID du portail captif.
Nom d'utilisateur	Nom d'utilisateur (ou ID invité) du client connecté.
Octets reçus	Nombre total d'octets reçus par le client.
Octets transmis	Nombre total d'octets transmis par le client.
Paquets DD reçus	Nombre total de paquets reçus par le client.
Paquets transmis	Nombre total de paquets transmis par le client.

Liste de contrôle d'accès

Les listes de contrôle d'accès (ACL) garantissent que seuls les utilisateurs autorisés peuvent accéder à des ressources spécifiques tout en bloquant toute tentative injustifiée d'atteindre des ressources réseau. Les listes de contrôle d'accès sont utilisées pour contrôler le flux de trafic, restreindre le contenu, décider quels types de trafic sont transférés ou bloqués et assurer la sécurité du réseau. Le commutateur prend en charge un total de 100 listes de contrôle d'accès, qui peuvent être une combinaison de listes de contrôle d'accès MAC, de listes de contrôle d'accès IPv4 de base, de listes de contrôle d'accès IPv4 étendues et de listes de contrôle d'accès IPv6.

Pour configurer un ACL :

1. Créez un ID ACL basé sur IPv4, IPv6 ou MAC.
2. Créez une règle et affectez informatique à un ID ACL unique.

3. Définissez les règles qui peuvent identifier les protocoles, les adresses IP et MAC source et de destination, ainsi que d'autres critères de correspondance de paquets.
4. Utilisez le numéro d'ID pour attribuer la liste de contrôle d'accès à un port ou à un lag. Pour afficher des exemples de configuration ACL, reportez-vous à la section Listes de contrôle d'accès (ACL) à la page 1183.

Utilisez l'Assistant ACL pour créer une ACL simple

L'Assistant ACL vous aide à créer une ACL simple et à l'appliquer facilement et rapidement aux ports sélectionnés. Tout d'abord, sélectionnez un type de liste de contrôle d'accès à utiliser lorsque vous créez une liste de contrôle d'accès. Ajoutez ensuite une règle ACL à cette ACL et appliquez-la aux ports sélectionnés.

❗ Remarque: Les étapes de la procédure suivante décrivent comment créer une liste de contrôle d'accès basée sur l'adresse MAC de destination. Si vous sélectionnez un autre type d'ACL (ou, par exemple, une ACL basée sur un IPv4 source), la page affiche des informations différentes.

Utilisez l'Assistant ACL pour créer une ACL

L'Assistant ACL permet de créer automatiquement une ACL en fonction d'un type d'ACL que vous devez sélectionner et des informations que vous devez fournir.

Pour utiliser l'Assistant ACL pour créer une ACL :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > ACL > Assistant ACL**.

ACL Type Selection

ACL Type ACL Based on Destination MAC

ACL Based on Destination MAC

☐	Sequence Number	Action	Match Every	Destination MAC	Destination MAC Mask	VLAN
☐						

Binding Configuration

Direction Inbound

Ports

Ports

1	3	5	7	9	11
2	4	6	8	10	12

LAG

LAG

1	3	5	7
2	4	6	8

Remarque: Les étapes de cette procédure décrivent la création d'une liste de contrôle d'accès basée sur l'adresse MAC de destination. Si vous sélectionnez un autre type de liste de contrôle d'accès, par exemple, une liste de contrôle d'accès basée sur une source IPv4, les éléments affichés sur cette page varient en fonction de l'étape en cours du processus de configuration des règles.

6. Dans le menu **type d'ACL**, sélectionnez le type d'ACL.

Vous pouvez sélectionner l'un des types de listes de contrôle d'accès suivants :

- **ACL basée sur l'adresse MAC de destination** : Crée une liste de contrôle d'accès basée sur l'adresse MAC de destination, le masque MAC de destination et l'VLAN.
- **ACL basée sur l'adresse MAC source** : Crée une liste de contrôle d'accès basée sur l'adresse MAC source, le masque MAC source et l'VLAN.

- **ACL basée sur IPv4 de destination** : Crée une liste de contrôle d'accès basée sur l'adresse IPv4 de destination et le masque d'adresse IPv4.
- **ACL basée sur IPv4 source** : Crée une liste de contrôle d'accès basée sur l'adresse IPv4 source et le masque d'adresse IPv4.
- **ACL basée sur IPv6 de destination** : Crée une ACL basée sur le préfixe IPv6 de destination et la longueur du préfixe IPv6.
- **ACL basée sur IPv6 source** : Crée une ACL basée sur le préfixe IPv6 source et la longueur du préfixe IPv6.
- **ACL basée sur le port L4 IPv4 de destination** : Crée une liste de contrôle d'accès basée sur le numéro de port IPv4 de la couche 4 de destination.
- **ACL basée sur le port source IPv4 L4** : Crée une liste de contrôle d'accès basée sur le numéro de port source IPv4 de couche 4.
- **ACL basée sur le port L4 IPv6 de destination** : Crée une liste de contrôle d'accès basée sur le numéro de port IPv6 de la couche 4 de destination.
- **ACL basée sur le port source IPv6 L4** : Crée une liste de contrôle d'accès basée sur le numéro de port source IPv6 de couche 4.

❗ **Remarque:** Pour les options de port L4, deux règles sont créées (une pour TCP et une pour UDP).

7. Dans le champ **numéro de séquence**, entrez un nombre entier compris entre 1 et 2147483647 qui est utilisé pour identifier la règle.
8. Dans le menu **action**, sélectionnez **autoriser** ou **refuser** pour spécifier l'action à effectuer si un paquet correspond aux critères de la règle.
9. Dans le menu **match Every**, sélectionnez l'une des options suivantes :
 - Faux Il n'est pas nécessaire que les paquets correspondent à la liste de contrôle d'accès et à la règle sélectionnées. Avec cette sélection, vous pouvez ajouter une adresse MAC de destination, un masque MAC de destination et un VLAN.
 - Vrai Tous les paquets doivent correspondre à la liste de contrôle d'accès et à la règle sélectionnées et sont autorisés ou refusés. Dans ce cas, puisque tous les paquets correspondent à la règle, l'option de configuration d'autres critères de correspondance n'est pas proposée.
10. Spécifiez les critères de correspondance supplémentaires pour le type de liste de contrôle d'accès sélectionné.

Les autres champs de critères de correspondance de règle disponibles pour la configuration dépendent du type de liste de contrôle d'accès sélectionné. Pour plus d'informations sur les champs de critères de correspondance possibles, reportez-vous au tableau suivant.

ACL basée sur	Champs
MAC destination	• MAC de destination : Spécifiez l'adresse MAC de destination à comparer à une trame Ethernet. Le format est xx:xx:xx:xx:xx:xx. Le mot clé BPDU peut être spécifié à l'aide d'une adresse MAC de destination 01:80:C2:xx:xx:xx. • Masque MAC de destination : Spécifiez le masque d'adresse MAC de destination, qui représente les bits de l'adresse MAC de destination à comparer à une trame Ethernet. Le format est xx:xx:xx:xx:xx:xx. Le mot clé BPDU peut être spécifié à l'aide d'un masque MAC de destination de 00:00:00:ff:ff:ff. • VLAN Spécifiez l'ID VLAN à faire correspondre dans la trame Ethernet.
Adresse MAC source	• MAC source : Spécifiez l'adresse MAC source à comparer avec une trame Ethernet. Le format est xx:xx:xx:xx:xx:xx. • Masque MAC source : Spécifiez le masque d'adresse MAC source, qui représente les bits de l'adresse MAC source à comparer à une trame Ethernet. Le format est (xx:xx:xx:xx:xx:xx). • VLAN Spécifiez l'ID VLAN à faire correspondre dans la trame Ethernet.
IPv4 de destination	• Adresse IP de destination. Spécifiez l'adresse IP de destination. • Masque IP de destination : Spécifiez le masque d'adresse IP de destination.
IPv4 source	• Adresse IP source Spécifiez l'adresse IP source. • Masque IP source : Spécifiez le masque d'adresse IP source.
IPv6 de destination	• Préfixe de destination : Spécifiez le préfixe de destination. • Longueur du préfixe de destination : Spécifiez la longueur du préfixe de destination.
IPv6 source	• Préfixe source : Spécifiez le préfixe de destination source. • Longueur du préfixe source : Spécifiez la longueur du préfixe source.
Port L4 IPv4 de destination	• Port L4 de destination (protocole): Spécifiez le protocole de port IPv4 L4 de destination. • Port L4 de destination (valeur): Spécifiez la valeur du port IPv4 L4 de destination.
Port source IPv4 L4	• Port source L4 (protocole): Spécifiez le protocole de port IPv4 L4 source. • Port source L4 (valeur): Spécifiez la valeur du port source IPv4 L4.
Port L4 IPv6 de destination	• Port L4 de destination (protocole): Spécifiez le protocole de port IPv6 L4 de destination. • Port L4 de destination (valeur): Spécifiez la valeur du port IPv6 L4 de destination.
Port source IPv6 L4	• Port source L4 (protocole): Spécifiez le protocole de port IPv6 L4 source. • Port source L4 (valeur): Spécifiez la valeur du port source IPv6 L4.

11. À titre d'exemple, les étapes suivantes décrivent comment créer une liste de contrôle d'accès basée sur l'adresse MAC de destination :
 - a. Dans le champ **MAC de destination**, spécifiez l'adresse MAC de destination qui doit être comparée aux informations d'une trame Ethernet.
Le format est xx:xx:xx:xx:xx:xx. Le mot clé BPDU peut être spécifié à l'aide d'une adresse MAC de destination 01:80:C2:xx:xx:xx.
 - b. Dans le champ **masque MAC de destination**, spécifiez le masque d'adresse MAC de destination qui doit être comparé aux informations d'une trame Ethernet.
Le format est xx:xx:xx:xx:xx:xx. Le mot clé BPDU peut être spécifié à l'aide d'un masque MAC de destination de 00:00:00:ff:ff:ff.
 - c. Dans le champ **ID VLAN**, spécifiez quel VLAN doit être comparé aux informations d'une trame Ethernet.
La plage est de 1 à 4093. Une plage VLAN ou VLAN peut être configurée.
12. Dans la section Configuration de la liaison, dans le menu **Direction**, sélectionnez la direction de filtrage des paquets pour la liste de contrôle d'accès.
 - Trafic entrant La liaison MAC peut être appliquée au trafic entrant uniquement.
 - **Sortant**: La liaison MAC peut être appliquée au trafic sortant uniquement.
13. Dans les tables ports et LAG de la section Configuration de liaison, sélectionnez les ports et LAG auxquels la liste de contrôle d'accès doit être appliquée.
Les ports du commutateur (unité 1) sont affichés. Si une pile est configurée, les ports de chaque commutateur empilé (unité 1, unité 2, etc.) sont affichés. En outre, tous les LAG sont affichés, qu'une pile soit configurée ou non.
14. Cliquez sur le bouton **Add** (Ajouter).
La règle est ajoutée à la liste de contrôle d'accès.
15. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
16. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Modifiez une règle ACL que vous avez créée avec l'Assistant ACL

Vous pouvez modifier une règle ACL que vous avez créée à l'aide de l'Assistant ACL.

Pour modifier une règle ACL que vous avez créée avec l'Assistant ACL :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > ACL > Assistant ACL**.

La page Assistant ACL s'affiche.

6. Cochez la case associée à la règle.

7. Mettez à jour les critères de correspondance si nécessaire.

8. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimez une règle ACL que vous avez créée avec l'Assistant ACL

Vous pouvez supprimer une règle ACL que vous avez créée avec l'Assistant ACL.

Pour supprimer une règle ACL que vous avez créée avec l'Assistant ACL :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > ACL > Assistant ACL**.

La page Assistant ACL s'affiche.

6. Cochez la case associée à la règle.

7. Cliquez sur le bouton **Supprimer**.

La règle est supprimée.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Exemple d'assistant ACL

Dans la figure suivante, la règle ACL est configurée pour vérifier les correspondances de paquets sur les ports 3, 7 et 8 et sur lag 4. Les paquets qui incluent une adresse source dans le réseau 203.0.113.0/24 peuvent être transmis par les interfaces. Tous les autres paquets sont abandonnés car chaque ACL inclut une règle implicite refuser tout comme dernière règle.

ACL Type Selection

ACL Type ACL Based on Source IPv4

ACL Based on Source IPv4

☐	Sequence Number	Action	Match Every	Source IP Address	Source IP Mask
	1	Permit	False	203.0.113.0	255.255.255.0

Binding Configuration

Direction Inbound

Ports

Ports	1	3	5	7	9	11
	☐	☒	☐	☒	☐	☐
	2	4	6	8	10	12
	☐	☐	☐	☒	☐	☐

LAG

LAG	1	3	5	7
	☐	☐	☐	☐
	2	4	6	8
	☐	☒	☐	☐

Pour plus d'informations sur l'Assistant ACL, reportez-vous à [Utilisez l'Assistant ACL pour créer une ACL simple](#) à la page 1029 la section .

Configurez une ACL MAC.

Une ACL MAC consiste en un ensemble de règles qui sont mises en correspondance séquentielle avec un paquet. Lorsqu'un paquet répond aux critères de correspondance d'une règle, l'action de règle spécifiée (autoriser ou refuser) est exécutée et les règles supplémentaires ne sont pas vérifiées pour une correspondance.

La définition d'une liste de contrôle d'accès MAC et l'application de informatique au commutateur impliquent plusieurs étapes :

1. Créez un ID ACL MAC (voir [Ajoutez une ACL MAC](#) à la page 1037).
2. Créez une règle MAC (voir [Configurer les règles ACL MAC](#) à la page 1040).
3. Associez la liste de contrôle d'accès MAC à une ou plusieurs interfaces (voir [Configurer les liaisons MAC](#) à la page 1045).

Vous pouvez afficher ou supprimer des configurations MAC ACL dans la table de liaison MAC (voir [Affichez ou supprimez les liaisons MAC ACL dans la table de liaison MAC](#) à la page 1047).

Ajoutez une ACL MAC

Vous pouvez ajouter une ACL MAC, après quoi vous pouvez ajouter une règle pour l'ACL MAC (voir [Ajoutez une règle pour une ACL MAC](#) à la page 1040).

Pour ajouter une ACL MAC :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez sécurité **sécurité > ACL > basique > ACL MAC**.

La page MAC ACL s'affiche.

La table MAC ACL affiche le nombre de ACL actuellement configurées sur le commutateur et le nombre maximal de ACL pouvant être configurées. La taille actuelle est égale au nombre de listes de contrôle d'accès IPv4 et IPv6 configurées plus le nombre de listes de contrôle d'accès MAC configurées.

6. Dans le champ **nom**, spécifiez un nom pour la liste de contrôle d'accès MAC.

La chaîne de nom peut contenir uniquement des caractères alphabétiques, numériques, tirets, traits de soulignement ou espaces. Le nom doit commencer par un caractère alphabétique.

7. Cliquez sur le bouton **Add** (Ajouter).

L'ACL MAC est ajoutée.

Chaque ACL configurée affiche les informations suivantes :

- **Règles** : Nombre de règles actuellement configurées pour la liste de contrôle d'accès MAC.
- Direction Sens du trafic de paquets affecté par la liste de contrôle d'accès MAC, qui peut être entrant ou vide. (Si la liste de contrôle d'accès n'est pas liée à une interface, la direction est vide.)

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Modifiez le nom d'une ACL MAC

Vous pouvez modifier le nom d'une ACL MAC.

Pour modifier le nom d'une ACL MAC :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > ACL > basique > ACL MAC**.

La page MAC ACL s'affiche.

6. Cochez la case associée à la liste de contrôle d'accès MAC.

7. Dans le champ **nom**, spécifiez le nouveau nom.

8. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimer une ACL MAC

Vous pouvez supprimer un ACL 802.1Q de base dont vous n'avez plus besoin.

Pour supprimer une ACL MAC :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur principale à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > ACL > basique > ACL MAC**.

La page MAC ACL s'affiche.

6. Cochez la case associée à la liste de contrôle d'accès MAC.

7. Cliquez sur le bouton **Supprimer**.

La liste de contrôle d'accès MAC est supprimée.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurer les règles ACL MAC .

Vous pouvez définir des règles pour les ACL basées sur MAC. La définition de liste d'accès comprend des règles qui spécifient si le trafic correspondant aux critères est transféré normalement ou rejeté. Une règle refuser tout par défaut est la dernière règle de chaque liste.

Ajoutez une règle pour une ACL MAC

Vous pouvez ajouter une règle pour une ACL MAC.

Pour ajouter une règle pour une ACL MAC :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **sécurité > ACL > basique > règles MAC**.

Rules

ACL Name:

Rule Table

☐	Sequence Number	Action	Assign Queue Id	Mirror Interface	Redirect Interface	Match Every	CoS	Destination MAC	Destination MAC Mask	EtherType Key	EtherType User Value	Source MAC
☐												

6. Dans le menu **nom de la liste de contrôle d'accès**, sélectionnez la liste de contrôle d'accès MAC.
7. Dans le champ **numéro de séquence**, entrez un nombre entier compris entre 1 et 2147483647 qui est utilisé pour identifier la règle.
8. Dans le menu **action**, sélectionnez l'action à effectuer si un paquet correspond aux critères de la règle :
 - **Permis** : Transfère les paquets qui répondent aux critères de la liste de contrôle d'accès.
 - Refuser Supprime les paquets qui répondent aux critères de la liste de contrôle d'accès.
9. Dans le champ **attribuer un ID de file d'attente**, spécifiez l'identificateur de file d'attente de sortie matérielle qui doit être utilisé pour traiter tous les paquets correspondant à cette règle ACL.
La plage de l'ID de file d'attente est comprise entre 0 et 6.
10. Dans le menu **Mirror interface**, sélectionnez l'interface de sortie vers laquelle le flux de trafic correspondant doit être copié, en plus d'être transféré normalement par le commutateur.
Ce champ ne peut pas être défini si une interface de redirection est déjà configurée pour la règle ACL. Ce champ est visible pour une action autoriser.
11. Dans le menu **Redirect interface**, sélectionnez l'interface de sortie vers laquelle le flux de trafic correspondant doit être redirigé, en contournant toute décision de transfert normalement prise par le commutateur.
Ce champ ne peut pas être défini si une interface miroir est déjà configurée pour la règle ACL.
12. Dans le menu **match Every**, indiquez si chaque paquet MAC de couche 2 doit être mis en correspondance avec la règle :

- Vrai Chaque paquet doit correspondre à la règle ACL sélectionnée.
 - Faux Tous les paquets ne doivent pas correspondre à la règle ACL sélectionnée.
13. Dans le champ **cos**, spécifiez la priorité 802.1p qui doit être comparée aux informations d'une trame Ethernet.
- La plage de priorité est comprise entre 0 et 7.
14. Dans le champ **MAC de destination**, spécifiez l'adresse MAC de destination qui doit être comparée aux informations d'une trame Ethernet.
- Le format est xx:xx:xx:xx:xx:xx. Le mot clé BPDU peut être spécifié à l'aide d'une adresse MAC de destination 01:80:C2:xx:xx:xx.
15. Dans le champ **masque MAC de destination**, spécifiez le masque d'adresse MAC de destination qui doit être comparé aux informations d'une trame Ethernet.
- Le format est xx:xx:xx:xx:xx:xx. Le mot clé BPDU peut être spécifié à l'aide d'un masque MAC de destination de 00:00:00:ff:ff:ff.
16. Dans le menu **clé EtherType**, sélectionnez la valeur EtherType à comparer aux informations d'une trame Ethernet.
- Les valeurs sont les suivantes :
- **Apple Talk**
 - **IBM SNA**
 - **IPv4**
 - **IPv6**
 - **IPX**
 - **MPLS Multicast**
 - **Monodiffusion MPLS**
 - **NETBIOS -**
 - **Novell**
 - **PPPoE**
 - **RARP**
 - **Valeur utilisateur**
17. Si vous sélectionnez **valeur utilisateur** dans le menu **clé EtherType**, dans le champ **valeur utilisateur EtherType**, spécifiez la valeur EtherType personnalisée à utiliser.
- Cette valeur doit être comparée aux informations contenues dans une trame Ethernet. La plage est comprise entre 0x0600 et 0xFFFF.
18. Dans le champ **MAC de destination**, spécifiez l'adresse MAC de destination qui doit être comparée aux informations d'une trame Ethernet.

Le format est xx:xx:xx:xx:xx:xx:xx.

19. Dans le champ **masque MAC de destination**, spécifiez le masque d'adresse MAC de destination qui doit être comparé aux informations d'une trame Ethernet.

Le format est xx:xx:xx:xx:xx:xx:xx.

20. Dans le champ **ID VLAN**, spécifiez quel VLAN doit être comparé aux informations d'une trame Ethernet.

La plage est de 1 à 4093. Vous pouvez configurer une plage VLAN unique ou VLAN.

21. Dans le menu **journalisation**, choisissez d'activer ou de désactiver la journalisation.

Cette option est disponible si la sélection dans le menu **action** est **refuser**.

Si vous sélectionnez **Activer**, la journalisation est activée pour cette règle ACL (sous réserve de la disponibilité des ressources sur le commutateur).

Si l'indicateur d'interruption de la liste d'accès est également activé, des interruptions périodiques sont générées, indiquant le nombre de fois que la règle a été évoquée pendant l'intervalle de rapport, qui est fixé à cinq minutes.

22. Dans le champ **débit de données conforme à la limite de débit**, spécifiez la valeur du débit de données conforme, qui correspond au débit de données auquel le trafic de confirmation est limité.

La plage est de 1 à 4294967295 secondes.

23. Dans le champ **Rate Limit Burst Size**, spécifiez la valeur de la taille de rafale, qui correspond à la taille à laquelle les rafales de trafic supérieures au débit de confirmation sont autorisées.

La plage est de 1 à 128 secondes.

24. Dans le menu **plage horaire**, sélectionnez le nom de la planification du minuteur en tant qu'option.

Pour plus d'informations sur les programmations de minuterie, reportez-vous à [Programmations de minuterie](#) à la page 247

Le champ État de la règle du tableau indique si la règle est active ou inactive. Vide signifie qu'aucun planning de minuterie n'est associé à la règle.

25. Cliquez sur le bouton **Add** (Ajouter).

La règle est ajoutée.

26. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Modifier les critères de correspondance d'une règle MAC

Vous pouvez modifier les critères de correspondance d'une règle MAC existante.

Pour modifier les critères de correspondance d'une règle MAC :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.
4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **sécurité > ACL > basique > règles MAC**.
La page règles MAC s'affiche.
6. Cochez la case associée à la règle.
7. Modifiez les champs si nécessaire.
8. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimer une règle d'une ACL MAC

Vous pouvez supprimer une règle d'une ACL MAC.

Pour supprimer une règle d'une adresse MAC :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.
4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **sécurité > ACL > basique > règles MAC**.
La page règles MAC s'affiche.
6. Cochez la case associée à la règle.
7. Cliquez sur le bouton **Supprimer**.
La règle est supprimée.
8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurer les liaisons MAC.

Lorsqu'une liste de contrôle d'accès est liée à une interface, toutes les règles définies sont appliquées à l'interface sélectionnée. Vous pouvez attribuer des ACL MAC aux interfaces et LAG.

Pour configurer la liaison MAC :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > ACL > basique > Configuration de liaison MAC**.

La page Configuration de la liaison MAC s'affiche.

6. Dans le menu **ID ACL**, sélectionnez une ACL.

7. Dans le menu **Direction**, sélectionnez la direction du trafic pour la liaison MAC :

- Trafic entrant La liaison MAC peut être appliquée au trafic entrant uniquement.
- **Sortant**: La liaison MAC peut être appliquée au trafic sortant uniquement.

8. Dans le champ **numéro de séquence**, spécifiez éventuellement un numéro pour indiquer l'ordre de la liste d'accès par rapport aux autres listes d'accès déjà affectées à l'interface et à la direction.

Un nombre faible indique un ordre de priorité élevé. Si un numéro de séquence est déjà utilisé pour l'interface et la direction, la liste d'accès spécifiée remplace la liste d'accès actuellement attachée utilisant ce numéro de séquence. Si vous ne spécifiez pas le numéro de séquence, un numéro de séquence supérieur d'un chiffre au

numéro de séquence le plus élevé actuellement utilisé pour l'interface et la direction est utilisé. La plage est de 1 à 4294967295.

9. Pour ajouter la liste de contrôle d'accès sélectionnée à un port ou à un lag, dans la table ports (ou, si une pile est configurée, dans l'une des tables ports) ou lag, cliquez sur le port ou le lag pour qu'une coche s'affiche.

Les tables ports et lag affichent les interfaces disponibles pour les liaisons ACL. Vous pouvez ajouter l'ACL à plusieurs ports et LAG.

Les ports du commutateur (unité 1) sont affichés. Si une pile est configurée, les ports de chaque commutateur empilé (unité 1, unité 2, etc.) sont affichés. En outre, tous les LAG sont affichés, qu'une pile soit configurée ou non.

10. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

11. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 182 : Informations sur l'état de liaison de l'interface

Champ	Description
Interface	L'interface sélectionnée.
Direction	Direction de filtrage des paquets sélectionnée pour la liste de contrôle d'accès.
Type de ACL	Type de liste de contrôle d'accès affecté à l'interface et à la direction sélectionnées.
ID ACL	Numéro ou nom de la liste de contrôle d'accès identifiant la liste de contrôle d'accès attribuée à l'interface et à la direction sélectionnées.
Numéro de séquence	Numéro de séquence indiquant l'ordre de la liste de contrôle d'accès spécifiée par rapport aux autres listes de contrôle d'accès affectées à l'interface et à la direction sélectionnées.

Affichez ou supprimez les liaisons MAC ACL dans la table de liaison MAC.

Vous pouvez afficher ou supprimer les liaisons MAC ACL dans la table de liaison MAC.

Pour afficher ou supprimer des liaisons ACL MAC :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à

[Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > ACL > basique > table de liaison**.

La page table de liaison s'affiche. Ce tableau affiche les liaisons MAC ACL-interface.

6. Pour supprimer une liaison MAC ACL-to-interface, procédez comme suit :

- a. Cochez la case en regard de l'interface.
- b. Cliquez sur le bouton **Supprimer**.

La liaison est supprimée.

7. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les informations affichées dans le tableau de liaison MAC.

Table 183 : Informations sur la table de liaison MAC

Champ	Description
Interface	Interface à laquelle l'ACL est liée.
Direction	Direction de filtrage des paquets sélectionnée pour la liste de contrôle d'accès.
Type de ACL	Type de liste de contrôle d'accès affecté à l'interface et à la direction sélectionnées.

Table 183 : Informations sur la table de reliure MAC (A continué)

Champ	Description
ID ACL	Nom de la liste de contrôle d'accès identifiant la liste de contrôle d'accès affectée à l'interface et à la direction sélectionnées.
Numéro de séquence	Numéro de séquence indiquant l'ordre de la liste de contrôle d'accès spécifiée par rapport aux autres listes de contrôle d'accès affectées à l'interface et à la direction sélectionnées.

Configurez une liste de contrôle d'accès IPv4 de base ou étendue.

Une liste de contrôle d'accès IPv4 consiste en un ensemble de règles qui sont mises en correspondance séquentielle avec un paquet. Lorsqu'un paquet répond aux critères de correspondance d'une règle, l'action de règle spécifiée (autoriser ou refuser) est exécutée et les règles supplémentaires ne sont pas vérifiées pour une correspondance. Vous devez spécifier les interfaces auxquelles s'applique une liste de contrôle d'accès IPv4, ainsi que si informatique s'applique au trafic entrant ou sortant.

La définition d'une liste de contrôle d'accès IPv4 et l'application de informatique au commutateur impliquent plusieurs étapes :

1. Ajoutez un ID ACL IPv4 (voir [Ajoutez une ACL IPv4](#) à la page 1050).

Les différences entre une liste de contrôle d'accès IPv4 de base et une liste de contrôle d'accès IPv4 étendue sont les suivantes :

- **ACL numérotée de 1 à 99** : Crée une liste de contrôle d'accès IPv4 de base, qui vous permet d'autoriser ou de refuser le trafic à partir d'une adresse IP source.
 - **ACL numérotée de 100 à 199** : Crée une liste de contrôle d'accès IPv4 étendue, qui vous permet d'autoriser ou de refuser des types spécifiques de trafic de couche 3 ou 4 d'une adresse IP source vers une adresse IP de destination. Ce type de liste de contrôle d'accès offre plus de granularité et de capacités de filtrage que la liste de contrôle d'accès IP de base.
 - **Liste de contrôle d'accès IP nommée** : Crée une liste de contrôle d'accès IPv4 étendue avec une chaîne de nom comportant jusqu'à 31 caractères alphanumériques. Le nom doit commencer par un caractère alphabétique.
2. Créez une règle IPv4 (voir [Configurer des règles pour une liste de contrôle d'accès IPv4 de base](#) à la page 1053 ou [Configurer des règles pour une ACL IPv4 étendue](#) à la page 1059).
 3. Associez la liste de contrôle d'accès IPv4 à une ou plusieurs interfaces (voir [Configurer les liaisons de l'interface ACL IP](#) à la page 1081).

Vous pouvez afficher ou supprimer des configurations IPv4 ACL dans la table de liaison IP ACL (voir [Affichez ou supprimez les liaisons IP ACL dans la table de liaison IP ACL](#), à la page 1083).

Ajoutez une ACL IPv4

Vous pouvez ajouter une liste de contrôle d'accès IPv4, après quoi vous pouvez ajouter une règle pour la liste de contrôle d'accès IPv4 (voir [Ajoutez une règle pour une ACL IPv4 de base](#) à la page 1054 ou [Ajoutez une règle pour une ACL IPv4 étendue](#) à la page 1059).

Pour ajouter une ACL IPv4 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > ACL > Avancé > IP ACL**.

La page IP ACL s'affiche.

La page IP ACL affiche la taille actuelle de la table ACL par rapport à la taille maximale de la table ACL. La taille actuelle est égale au nombre de listes de contrôle d'accès IPv4 configurées plus le nombre de listes de contrôle d'accès MAC et IPv6

configurées. Le nombre maximum de listes de contrôle d'accès sur le commutateur est de 100.

Le champ nombre actuel de listes de contrôle d'accès affiche le nombre actuel de toutes les listes de contrôle d'accès configurées sur le commutateur.

Le champ ACL maximum affiche le nombre maximal de ACL que vous pouvez configurer sur le commutateur.

6. Dans le champ **ID de la liste de contrôle d'accès IP**, spécifiez l'ID ou le nom de la liste de contrôle d'accès IP, qui dépend du type de liste de contrôle d'accès IP. L'ID de la liste de contrôle d'accès IP est un entier compris dans la plage suivante :
 - 199 Crée une liste de contrôle d'accès IP de base, qui vous permet d'autoriser ou de refuser le trafic à partir d'une adresse IP source.
 - 100199 Crée une liste de contrôle d'accès IP étendue, qui vous permet d'autoriser ou de refuser des types spécifiques de trafic de couche 3 ou 4 d'une adresse IP source vers une adresse IP de destination. Ce type de liste de contrôle d'accès offre plus de granularité et de capacités de filtrage que la liste de contrôle d'accès IP standard.
 - **Nom IP ACL** : Crée une liste de contrôle d'accès IP étendue avec une chaîne de nom comportant jusqu'à 31 caractères alphanumériques. Le nom doit commencer par un caractère alphabétique.

Chaque ACL configurée affiche les informations suivantes :

- **Règles** : Nombre de règles actuellement configurées pour la liste de contrôle d'accès IPv4.
 - **Type** : Identifie la liste de contrôle d'accès comme une liste de contrôle d'accès IP de base (avec un ID compris entre 1 et 99), une liste de contrôle d'accès IP étendue (avec un ID compris entre 100 et 199) ou une liste de contrôle d'accès nommée (qui est également une liste de contrôle d'accès étendue).
7. Cliquez sur le bouton **Add** (Ajouter).

L'ACL IP est ajoutée.
 8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Modifiez le numéro ou le nom d'une liste de contrôle d'accès IPv4

Vous pouvez modifier le numéro ou le nom d'une liste de contrôle d'accès IPv4.

Pour modifier le numéro ou le nom d'une liste de contrôle d'accès IPv4 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > ACL > Avancé > IP ACL**.

L'écran IP Configuration (Configuration IP) s'affiche.

6. Cochez la case associée à la liste de contrôle d'accès IP.

7. Dans le champ **IP ACL**, spécifiez le nouveau numéro ou nom.

8. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimer une ACL IPv4

Vous pouvez supprimer un ACL IPv4 avancé dont vous n'avez plus besoin.

Pour supprimer une ACL IPv4 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > ACL > Avancé > IP ACL**.

L'écran IP Configuration (Configuration IP) s'affiche.

6. Cochez la case associée à la liste de contrôle d'accès IP.

7. Cliquez sur le bouton **Supprimer**.

L'ACL IP est supprimée.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurer des règles pour une liste de contrôle d'accès IPv4 de base .

Vous pouvez définir des règles pour les ACL standard basées sur IP (ACL de base). La définition de liste d'accès comprend des règles qui spécifient si le trafic correspondant aux critères est transféré normalement ou rejeté.

❗ **Remarque:** Une règle de refus implicite est incluse à la fin d'une liste ACL. Cela signifie que si une liste de contrôle d'accès est appliquée à un paquet, et si aucune des règles explicites ne correspond, alors la dernière règle implicite refuser tout s'applique et le paquet est abandonné.

Ajoutez une règle pour une ACL IPv4 de base

Vous pouvez ajouter une règle pour une ACL IPv4 de base.

Pour ajouter une règle pour une ACL IPv4 de base :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

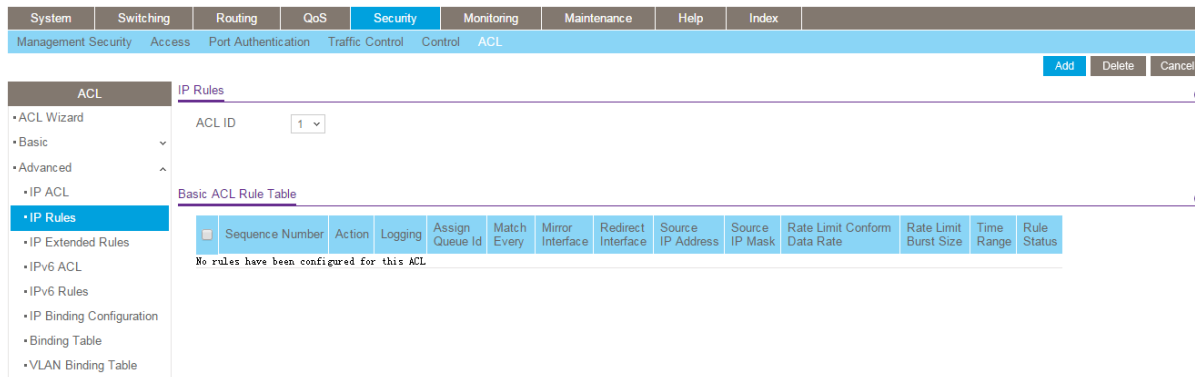
- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur principale à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > ACL > Avancé > règles IP**.



S'il n'existe aucune règle, le tableau des règles de l'ACL de base affiche le message *aucune règle n'a été configurée pour cette ACL*. S'il existe une ou plusieurs règles pour l'ACL, elles s'affichent dans le tableau des règles de l'ACL de base.

6. Dans le menu **ID ACL**, sélectionnez l'ACL IP pour laquelle vous souhaitez ajouter ou modifier une règle.

Pour les listes de contrôle d'accès IP de base, il doit s'agir d'un ID compris entre 1 et 99.

7. Cliquez sur le bouton **Add** (Ajouter).

La page qui s'affiche vous permet de configurer la règle ACL de base (standard).

8. Spécifiez les critères de correspondance suivants pour la règle :

- **Numéro de séquence** : Entrez un numéro de séquence ACL compris entre 1 et 2147483647 utilisé pour identifier la règle. Une liste de contrôle d'accès IP peut contenir jusqu'à 50 règles.
- **Action** : Sélectionnez l'action de transfert ACL, qui est l'une des actions suivantes :
 - **Permis** : Transférer les paquets qui répondent aux critères de la liste de contrôle d'accès.

File d'attente de sortie : Si la sélection dans le menu **action** est **autoriser**, vous pouvez spécifier l'identificateur de file d'attente de sortie matérielle utilisé pour traiter tous les paquets correspondant à cette règle de liste de contrôle d'accès IP. La plage d'ID de file d'attente est comprise entre 0 et 6.

- Refuser Abandonner les paquets qui répondent aux critères de la liste de contrôle d'accès.

Enregistrement... Si la sélection dans le menu **action** est **refuser**, vous pouvez activer la journalisation pour la liste de contrôle d'accès en sélectionnant le bouton radio **Activer**. (La journalisation dépend de la disponibilité des ressources sur le commutateur.)

- **Correspondre tous les** : Sélectionnez l'un des boutons radio pour spécifier si tous les paquets doivent correspondre à la règle ACL IP sélectionnée :

- Activer. Tous les paquets doivent correspondre à la liste de contrôle d'accès et à la règle sélectionnées et sont autorisés ou refusés.
- Désactiver : Tous les paquets ne doivent pas correspondre à la règle ACL IP sélectionnée.

- **Interface miroir** : Dans le menu, sélectionnez l'interface de sortie vers laquelle le flux de trafic correspondant doit être copié, en plus d'être transféré normalement par le commutateur.

Vous pouvez sélectionner une interface miroir ou une interface de redirection. Ces options s'excluent mutuellement.

- **Interface de redirection** : Dans le menu, sélectionnez l'interface de sortie vers laquelle le flux de trafic correspondant doit être redirigé, en contournant toute décision de transfert normalement prise par le commutateur.

Vous pouvez sélectionner une interface de redirection ou une interface miroir. Ces options s'excluent mutuellement.

- **Adresse IP SRC** : Spécifiez une adresse IP à l'aide de la notation décimale à points à comparer à l'adresse IP source d'un paquet comme critère de correspondance pour la règle de liste de contrôle d'accès IP sélectionnée.
- **Masque IP SRC** : Spécifiez le masque IP en notation décimale à points à utiliser avec l'adresse IP source.
- **Limite de débit conforme débit de données** : Spécifiez la valeur du débit de données conforme, qui correspond au débit auquel le trafic de confirmation est limité. La plage est de 1 à 4294967295 secondes.
- **Taille de rafale limite de débit** : Spécifiez la valeur de la taille des rafales, qui correspond à la taille à laquelle les rafales de trafic supérieures au débit de confirmation sont autorisées. La plage est de 1 à 128 secondes.
- **Plage de temps** Dans le menu **plage horaire**, sélectionnez le planning de minuterie qui doit être associé à la règle. Pour plus d'informations sur les programmations de minuterie, reportez-vous à la section [Programmations de minuterie](#) à la page 247. Si vous n'avez configuré aucun programme de minuterie, le menu ne présente aucune option.

9. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

Le champ État de la règle du tableau indique si la règle est active ou inactive. Vide signifie qu'aucun planning de minuterie n'est associé à la règle.

10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Modifiez les critères de correspondance d'une règle de liste de contrôle d'accès IPv4 de base

Vous pouvez modifier les critères de correspondance d'une règle de liste de contrôle d'accès IPv4 de base.

Pour modifier les critères de correspondance d'une règle ACL IPv4 de base :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > ACL > Avancé > règles IP**.

La page règles IP s'affiche.

6. Dans le menu **ID ACL**, sélectionnez l'ACL qui inclut la règle à modifier.

7. Dans le tableau des règles de l'ACL de base, cliquez sur la règle.

La règle est un lien hypertexte. La page Configuration des règles d'ACL standard s'affiche.

8. Modifiez les critères de base de la règle ACL IP.

9. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimer une règle de liste de contrôle d'accès IPv4 de base

Vous pouvez supprimer un ACL IPv4 de base dont vous n'avez plus besoin.

Pour supprimer une règle ACL IPv4 de base :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > ACL > Avancé > règles IP**.

La page règles IP s'affiche.

6. Dans le menu **ID ACL**, sélectionnez l'ACL qui inclut la règle à modifier.
7. Dans la table de règles de base de l'ACL, cochez la case associée à la règle.
8. Cliquez sur le bouton **Supprimer**.

La règle est supprimée.

9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurer des règles pour une ACL IPv4 étendue .

Vous pouvez définir des règles pour les ACL IPv4 étendues. La définition de liste d'accès comprend des règles qui spécifient si le trafic correspondant aux critères est transféré normalement ou rejeté.

❗ Remarque: Une règle de refus implicite est incluse à la fin d'une liste ACL. Cela signifie que si une liste de contrôle d'accès est appliquée à un paquet et si aucune des règles explicites ne correspond, alors la dernière règle implicite refuser tout s'applique et le paquet est abandonné.

Ajoutez une règle pour une ACL IPv4 étendue

Vous pouvez ajouter une règle pour une ACL IPv4 étendue.

Pour ajouter une règle pour une ACL IPv4 étendue :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

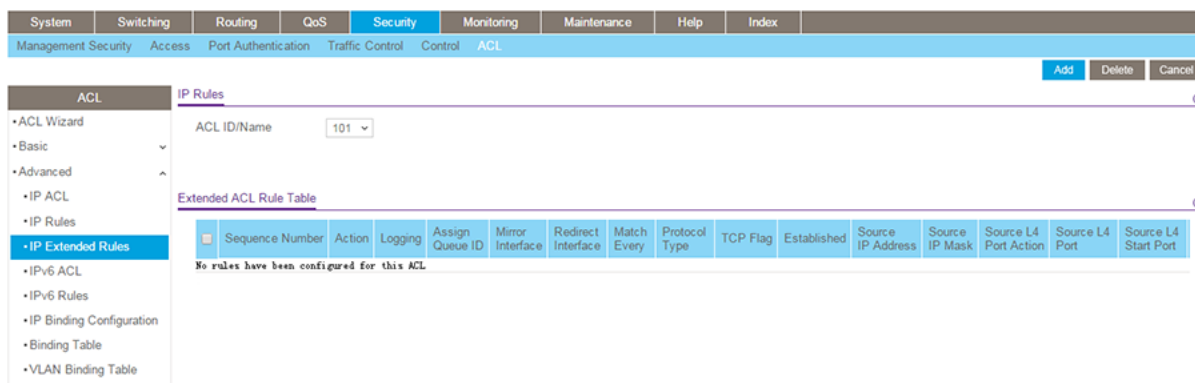
- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **sécurité > ACL > Avancé > règles IP étendues**.



S'il n'existe aucune règle, le tableau des règles ACL étendues affiche le message *aucune règle n'a été configurée pour cette ACL*. S'il existe une ou plusieurs règles pour la liste de contrôle d'accès, les règles s'affichent dans le tableau des règles de la liste de contrôle d'accès étendue.

6. Dans le menu **ID/nom de la LCA**, sélectionnez la LCA IP pour laquelle vous souhaitez ajouter une règle.

Pour les listes de contrôle d'accès IP étendues, il doit s'agir d'un ID compris entre 101 et 199 ou d'un nom.

7. Cliquez sur le bouton **Add** (Ajouter).
La page qui s'affiche vous permet de configurer la règle étendue.
8. Configurez les options suivantes pour la règle :

- **Numéro de séquence** : Entrez un nombre compris entre 1 et 2147483647 qui sera utilisé pour identifier la règle. Une liste de contrôle d'accès IP étendue peut contenir jusqu'à 1023 règles.
- **Action** : Sélectionnez l'action de transfert ACL, qui est l'une des actions suivantes :
 - **Permis** : Transférer les paquets qui répondent aux critères de la liste de contrôle d'accès.
 - **File d'attente de sortie** : Si la sélection dans le menu **action** est **autoriser**, sélectionnez l'identificateur de file d'attente de sortie matériel utilisé pour traiter tous les paquets correspondant à cette règle de liste de contrôle d'accès IP. La plage d'ID de file d'attente est comprise entre 0 et 6.
 - Refuser Abandonner les paquets qui répondent aux critères de la liste de contrôle d'accès.

Cette option est disponible si la sélection dans le menu **action** est **refuser**.

Si vous sélectionnez **Activer**, la journalisation est activée pour cette règle ACL (sous réserve de la disponibilité des ressources sur le commutateur).

Si l'indicateur d'interruption de la liste d'accès est également activé, des interruptions périodiques sont générées, indiquant le nombre de fois que la règle a été évoquée pendant l'intervalle de rapport, qui est fixé à cinq minutes.

- Interface Pour une action autoriser, utilisez une interface miroir ou une interface de redirection :
 - Sélectionnez le bouton radio **miroir** et utilisez le menu pour spécifier l'interface de sortie vers laquelle le flux de trafic correspondant est copié, en plus d'être transféré normalement par l'unité.
 - Sélectionnez le bouton radio **redirection** et utilisez le menu pour spécifier l'interface de sortie vers laquelle le flux de trafic correspondant est forcé, en contournant toute décision de transfert normalement prise par le périphérique.
 - **Correspondre tous les** : Sélectionnez l'un des boutons radio pour spécifier si tous les paquets doivent correspondre à la règle ACL IP sélectionnée :
 - Faux Tous les paquets ne doivent pas correspondre à la règle ACL IP sélectionnée. Vous pouvez configurer d'autres critères de correspondance sur la page.
 - Vrai Tous les paquets doivent correspondre à la liste de contrôle d'accès et à la règle sélectionnées et sont autorisés ou refusés. Dans ce cas, vous ne pouvez pas configurer d'autres critères de correspondance sur la page.
 - **Type de protocole** : Dans le menu, sélectionnez un protocole auquel le protocole IP d'un paquet doit correspondre : **IP, ICMP, IGMP, TCP, UDP, EIGRP, GRE, IPINIP, OSPF, PIM** ou **autre**. Si vous sélectionnez **autre**, entrez un numéro de protocole compris entre 0 et 255.
 - **Drapeau TCP** : Si vous sélectionnez **TCP** dans le menu **type de protocole**, pour chaque indicateur TCP, vous pouvez spécifier si l'indicateur TCP d'un paquet doit correspondre ou non. Les valeurs des indicateurs TCP sont URG, ACK, PSH, RST, SYN et fin. Vous pouvez définir chaque indicateur TCP séparément sur l'une des options suivantes :
 - Ignorer Le drapeau TCP du paquet est ignoré. Il s'agit de l'option par défaut.
 - Appliquer Un paquet correspond à cette règle ACL si l'indicateur TCP de ce paquet est défini.
 - **Clear** (Effacer) - Un paquet correspond à cette règle ACL si l'indicateur TCP de ce paquet n'est pas défini.
- ❗ **Remarque**: Si les drapeaux RST et ACK sont définis, l'option **Established** est disponible, indiquant qu'une correspondance se produit si les bits spécifiés par RST ou ACK sont définis dans l'en-tête du paquet.

- **SRC** : Dans le champ **SRC**, entrez une adresse IP source, en utilisant la notation décimale à points, à comparer à l'adresse IP source d'un paquet comme critère de correspondance pour la règle ACL IP sélectionnée :
 - Si vous sélectionnez le bouton radio **adresse IP**, entrez une adresse IP ou une plage d'adresses IP. Vous pouvez saisir un masque générique approprié pour appliquer ce critère. Si ce champ est laissé vide, informatique signifie any.
 - Si vous sélectionnez le bouton radio **hôte**, le masque générique est configuré en tant que 0,0,0,0. Si ce champ est laissé vide, informatique signifie any.

Le masque générique détermine quels bits sont utilisés et quels bits sont ignorés. Un masque générique de 0.0.0.0 indique qu'aucun des bits n'est important. Un caractère générique de 255.255.255.255 indique que tous les bits sont importants.
- **SRC L4** : Les options ne sont disponibles que si la sélection dans le menu **type de protocole** est **TCP** ou **UDP**. Utilisez l'option de port L4 source pour spécifier les conditions correspondantes pertinentes pour les numéros de port L4 dans la règle ACL étendue.

Vous pouvez sélectionner le bouton radio **Port** ou le bouton radio **plage** :

- **Port**. Si vous sélectionnez le bouton radio Port, vous pouvez entrer le numéro de port vous-même ou sélectionner l'un des protocoles suivants dans le menu :
 - Les protocoles de port TCP IP source sont **Domain**, **Echo**, **FTP**, **FTP**, **FTP data**, **www-http**, **SMTP**, **Telnet**, **POP2**, **POP3** et **BGP**.
 - Les protocoles de port UDP IP source sont **Domain**, **Echo**, **SNMP**, **NTP**, **RIP**, **heure**, **OMS** et **TFTP**.

Chacune de ces valeurs se traduit par son numéro de port équivalent, qui est utilisé à la fois comme début et fin de la plage de ports.

Sélectionnez autre dans le menu pour entrer un numéro de port. Si vous sélectionnez autre dans le menu mais laissez le champ vide, informatique signifie tout.

Les conditions de correspondance pertinentes pour les numéros de port L4 sont les suivantes :

- **Égal à** : La règle ACL IP correspond si le numéro de port source de couche 4 est égal au numéro de port ou à la clé de port spécifié.
- **Différent** : La règle ACL IP correspond si le numéro de port source de couche 4 n'est pas égal au numéro de port ou à la clé de port spécifié.

- **Inférieur à** : La règle ACL IP correspond si le numéro de port source de couche 4 est inférieur au numéro de port ou à la clé de port spécifié.
- **Supérieur à** : La règle ACL IP correspond si le numéro de port source de couche 4 est supérieur au numéro de port ou à la clé de port spécifiés.
- o **Portée** : Si vous sélectionnez le bouton radio plage, la règle ACL IP correspond uniquement si le numéro de port source de couche 4 se trouve dans la plage de ports spécifiée. Le port de départ, le port de fin et tous les ports intermédiaires font partie de la plage de ports de couche 4.

Les champs **Port de début** et **Port de fin** identifient le premier et le dernier port faisant partie de la plage de ports. Cette valeur doit être comprise entre 0 et 65535.

Vous pouvez entrer vous-même la plage de ports ou sélectionner l'un des protocoles suivants dans le menu :

- Les protocoles de port TCP IP source sont **Domain, Echo, FTP, FTP, FTP data, www-http, SMTP, Telnet, POP2, POP3** et **BGP**.
- Les protocoles de port UDP IP source sont **Domain, Echo, SNMP, NTP, RIP, heure, OMS** et **TFTP**.

Chacune de ces valeurs se traduit par son numéro de port équivalent, qui est utilisé à la fois comme début et fin de la plage de ports. Sélectionnez autre dans le menu pour entrer un numéro de port. Si vous sélectionnez autre dans le menu mais laissez le champ vide, informatique signifie tout.

Le masque générique détermine quels bits sont utilisés et quels bits sont ignorés. Un masque générique de 0.0.0.0 indique qu'aucun des bits n'est important. Un caractère générique de 255.255.255.255 indique que tous les bits sont importants.

- **DST** : Dans le champ **DST**, entrez une adresse IP de destination, en utilisant la notation décimale à points, à comparer à l'adresse IP de destination d'un paquet comme critère de correspondance pour la règle ACL IP sélectionnée :
 - o Si vous sélectionnez le bouton radio **adresse IP**, entrez une adresse IP avec un masque générique approprié pour appliquer ce critère. Si ce champ est laissé vide, informatique signifie any.
 - o Si vous sélectionnez le bouton radio **hôte**, le masque générique est configuré en tant que 0,0.0,0. Si ce champ est laissé vide, informatique signifie any.

Le masque générique détermine quels bits sont utilisés et quels bits sont ignorés. Un masque générique de 0.0.0.0 indique qu'aucun des bits n'est important. Un caractère générique de 255.255.255.255 indique que tous les bits sont importants.

- **DST L4** : Les options ne sont disponibles que si la sélection dans le menu **type de protocole** est **TCP** ou **UDP**. Utilisez l'option de port L4 de destination pour

spécifier les conditions correspondantes pertinentes pour les numéros de port L4 dans la règle ACL étendue.

Vous pouvez sélectionner le bouton radio **Port** ou le bouton radio **plage** :

- **Port.** Si vous sélectionnez le bouton radio Port, vous pouvez entrer le numéro de port vous-même ou sélectionner l'un des protocoles suivants dans le menu.
 - Les protocoles de port TCP IP de destination sont **domaine, Echo, FTP, données FTP, www-http, SMTP, Telnet, POP2, POP3** et **BGP**.
 - Les protocoles de port UDP IP de destination sont **Domain, Echo, SNMP, NTP, RIP, heure, OMS** et **TFTP**.

Chacune de ces valeurs se traduit par son numéro de port équivalent, qui est utilisé à la fois comme début et fin de la plage de ports.

Sélectionnez autre dans le menu pour entrer un numéro de port. Si vous sélectionnez autre dans le menu mais laissez le champ vide, informatique signifie tout.

Les conditions de correspondance pertinentes pour les numéros de port L4 sont les suivantes :

- **Égal à** : La règle ACL IP correspond si le numéro de port source de couche 4 est égal au numéro de port ou à la clé de port spécifié.
- **Différent** : La règle ACL IP correspond si le numéro de port source de couche 4 n'est pas égal au numéro de port ou à la clé de port spécifié.
- **Inférieur à** : La règle ACL IP correspond si le numéro de port source de couche 4 est inférieur au numéro de port ou à la clé de port spécifié.
- **Supérieur à** : La règle ACL IP correspond si le numéro de port source de couche 4 est supérieur au numéro de port ou à la clé de port spécifiés.
- **Portée** : Si vous sélectionnez le bouton radio plage, la règle ACL IP correspond uniquement si le numéro de port de destination de couche 4 se trouve dans la plage de ports spécifiée. Le port de départ, le port de fin et tous les ports intermédiaires font partie de la plage de ports de couche 4.

Les champs **Port de début** et **Port de fin** identifient le premier et le dernier port faisant partie de la plage de ports. Ces valeurs peuvent aller de 0 à 65535. Vous pouvez sélectionner vous-même la plage de ports ou sélectionner l'un des protocoles suivants dans le menu :

- Les protocoles de port TCP IP de destination sont **domaine, Echo, FTP, données FTP, www-http, SMTP, Telnet, POP2, POP3** et **BGP**.
- Les protocoles de port UDP IP de destination sont **Domain, Echo, SNMP, NTP, RIP, heure, OMS** et **TFTP**.

Chacune de ces valeurs se traduit par son numéro de port équivalent, qui est utilisé à la fois comme début et fin de la plage de ports.

Sélectionnez autre dans le menu pour entrer un numéro de port. Si vous sélectionnez autre dans le menu mais laissez le champ vide, informatique signifie tout.

Le masque générique détermine quels bits sont utilisés et quels bits sont ignorés. Un masque générique de 0.0.0.0 indique qu'aucun des bits n'est important. Un caractère générique de 255.255.255.255 indique que tous les bits sont importants.

- **Type IGMP** : Si vous sélectionnez **IGMP** dans le menu **type de protocole** et que vous spécifiez le type IGMP, la règle IP ACL correspond au type de message IGMP spécifié. La plage est de 0 à 255. Si ce champ est laissé vide, informatique signifie any.
 - **ICMP** : Si vous sélectionnez **ICMP** dans le menu **type de protocole**, vous pouvez sélectionner le bouton radio **type** ou **message** :
 - Si vous sélectionnez le bouton radio **type**, notez les points suivants :
 - Les champs **type** et **Code** sont activés uniquement si le protocole est ICMP. Utilisez ces champs pour spécifier une condition de correspondance pour les paquets ICMP :
 - Si vous spécifiez des informations dans le champ **type**, la règle ACL IP correspond au type de message ICMP spécifié. La plage de numéros de port peut être comprise entre 0 et 255.
 - Si vous spécifiez des informations dans le champ **Code**, la règle ACL IP correspond au code de message ICMP spécifié. Le code peut être compris entre 0 et 255.
 - Si ces champs sont laissés vides, informatique signifie any.
 - Si vous sélectionnez le bouton radio **message**, dans le menu, sélectionnez le type de message ICMP à faire correspondre à la règle IP ACL sélectionnée. La spécification d'un type de message implique que le type ICMP et le code ICMP sont spécifiés. Le message ICMP est décodé dans le type ICMP correspondant et le code ICMP dans le type ICMP.
- Les types de message IPv4 ICMP sont **Echo, écho-réponse, host-redirect, mobile-redirect, net-redirect, net-inaccessible, redirect, paquet-trop-gros, port-inaccessible, quench-source, sollicitation-routeur, annonce-routeur, TTL-dépassé, temps dépassé** et **inaccessible**.
- fragmentée Sélectionnez le bouton radio **Activer** pour autoriser les fragments initiaux (c'est-à-dire que le bit de fragment est confirmé) ou laissez le bouton radio **désactiver** par défaut sélectionné pour empêcher l'utilisation des fragments initiaux.

Cette option n'est pas valide pour les règles qui correspondent à des informations L4 telles qu'un numéro de port TCP, car ces informations sont transportées dans le paquet initial.

- Type de service Sélectionnez une condition de correspondance de type de service pour la règle ACL IP étendue.

Les valeurs possibles sont **IP DSCP**, **IP précedence** et **IP TOS**, qui sont des méthodes alternatives pour spécifier un critère de correspondance pour le même champ de type de service dans l'en-tête IP. Chaque méthode utilise une notation utilisateur différente. Après avoir effectué une sélection, vous pouvez spécifier les valeurs appropriées.

- **IP DSCP** : Il s'agit d'une configuration facultative. Spécifiez le champ IP DiffServ Code point (DSCP). Le DSCP est défini comme les 6 bits de poids fort de l'octet de type de service dans l'en-tête IP. Entrez un entier compris entre 0 et 63. Pour sélectionner le DSCP IP, sélectionnez l'un des mots-clés DSCP dans le menu. Pour spécifier une valeur numérique, sélectionnez autre. Un champ s'affiche dans lequel vous pouvez entrer la valeur numérique du DSCP.
- **Priorité IP** : Il s'agit d'une configuration facultative. Le champ de priorité IP dans un paquet est défini comme les trois bits de poids fort de l'octet de type de service dans l'en-tête IP. Entrez un entier compris entre 0 et 7.
- **IP TOS** : Il s'agit d'une configuration facultative. Le champ IP ToS dans un paquet est défini comme les 8 bits de l'octet de type de service dans l'en-tête IP. La valeur des bits ToS est un nombre hexadécimal compris entre 00 et 09 et entre aa et F. La valeur du masque ToS est un nombre hexadécimal compris entre 00 et FF. Le masque ToS indique les positions de bits dans la valeur de bits ToS qui sont utilisées pour la comparaison avec le champ ToS IP dans un paquet.

Par exemple, pour rechercher une valeur ToS IP pour laquelle le bit 7 est défini et est la valeur la plus significative, pour laquelle le bit 5 est défini et pour laquelle le bit 1 est effacé, utilisez une valeur de bits ToS de 0xA0 et un masque ToS de 0xFF.

- **Limite de débit conforme débit de données** : Spécifiez la valeur du débit de données conforme, qui correspond au débit auquel le trafic de confirmation est limité. La plage est de 1 à 4294967295 secondes.
- **Taille de rafale limite de débit** : Spécifiez la valeur de la taille des rafales, qui correspond à la taille à laquelle les rafales de trafic supérieures au débit de confirmation sont autorisées. La plage est de 1 à 128 secondes.
- Plage de temps Dans le menu **plage horaire**, sélectionnez le planning de minuterie qui doit être associé à la règle. Pour plus d'informations sur les programmations de minuterie, reportez-vous à la section Programmations de minuterie à la page 247. Si vous n'avez configuré aucun programme de minuterie, le menu ne présente aucune option.

9. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

Le champ État de la règle du tableau indique si la règle est active ou inactive. Vide signifie qu'aucun planning de minuterie n'est associé à la règle.

10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Modifiez les critères de correspondance pour une règle ACL IPv4 étendue

Vous pouvez modifier les critères de correspondance d'une règle ACL IPv4 étendue.

Pour modifier les critères de correspondance d'une règle ACL IPv4 étendue existante :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > ACL > Avancé > règles IP étendues**.

La page IP Extended Rules s'affiche.

6. Dans le menu **ID/nom de l'ACL**, sélectionnez l'ACL qui inclut la règle à modifier.

7. Dans le tableau des règles ACL étendues, cliquez sur la règle.

La règle est un lien hypertexte. La page Configuration des règles ACL étendues s'affiche.

8. Modifiez les critères de la règle ACL IP étendue.

9. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimez une règle ACL IPv4 étendue

Vous pouvez supprimer un ACL IPv4 avancé dont vous n'avez plus besoin.

Pour supprimer une règle ACL IPv4 étendue :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > ACL > Avancé > règles IP étendues**.

La page IP Extended Rules s'affiche.

6. Dans le menu **ID/nom de la liste de contrôle d'accès**, sélectionnez la liste de contrôle d'accès qui inclut la règle à supprimer.
7. Dans le tableau des règles ACL étendues, cochez la case associée à la règle.
8. Cliquez sur le bouton **Supprimer**.
La règle est supprimée.
9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez une liste de contrôle d'accès IPv6

.

Une liste de contrôle d'accès IPv6 consiste en un ensemble de règles qui sont mises en correspondance séquentielle avec un paquet. Lorsqu'un paquet répond aux critères de correspondance d'une règle, l'action de règle spécifiée (autoriser ou refuser) est exécutée et les règles supplémentaires ne sont pas vérifiées pour une correspondance. Vous devez spécifier les interfaces auxquelles s'applique une liste de contrôle d'accès IPv6, ainsi que si informatique s'applique au trafic entrant ou sortant.

La définition d'une liste de contrôle d'accès IPv6 et l'application de informatique au commutateur impliquent plusieurs étapes :

1. Ajoutez un ID ACL IPv6 (voir [Ajoutez une ACL IPv6](#) à la page 1069).
Une liste de contrôle d'accès IPv6 doit commencer par une chaîne de nom comportant jusqu'à 31 caractères alphanumériques. Le nom doit commencer par un caractère alphabétique.
2. Créez une règle IPv6 (voir [Configurer des règles pour une ACL IPv6](#) à la page 1073).
3. Associez la liste de contrôle d'accès IPv6 à une ou plusieurs interfaces (voir [Configurer les liaisons de l'interface ACL IP](#) à la page 1081).

Vous pouvez afficher ou supprimer des configurations IPv6 ACL dans la table de liaison IP ACL (voir [Affichez ou supprimez les liaisons IP ACL dans la table de liaison IP ACL](#) à la page 1083).

Ajoutez une ACL IPv6

Vous pouvez ajouter une liste de contrôle d'accès IPv6, après quoi vous pouvez ajouter une règle pour la liste de contrôle d'accès IPv6 (voir [Ajoutez une règle pour une ACL IPv6](#) à la page 1073).

Pour ajouter une ACL IPv6 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > ACL > Avancé > ACL IPv6**.

La page ACL IPv6 s'affiche.

6. Dans le champ **liste de contrôle d'accès IPv6**, spécifiez un nom pour identifier la liste de contrôle d'accès IPv6.

Il s'agit de la chaîne de nom IPv6 ACL, qui comprend jusqu'à 31 caractères alphanumériques uniquement. Le nom doit commencer par un caractère alphabétique.

7. Cliquez sur le bouton **Add** (Ajouter).

L'ACL IPv6 est ajoutée à la configuration du commutateur.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 184 : Informations ACL IPv6

Champ	Description
Numéro actuel de liste de contrôle d'accès	Nombre actuel de listes de contrôle d'accès configurées sur le commutateur.
ACL maximum	Nombre maximal de listes de contrôle d'accès IP pouvant être configurées sur le commutateur.
Règles	Nombre maximal de listes de contrôle d'accès pouvant être configurées sur le commutateur.
Type	Le type est IPv6 ACL.

Modifiez le nom d'une liste de contrôle d'accès IPv6

Vous pouvez modifier le nom d'une liste de contrôle d'accès IPv6.

Pour modifier le nom d'une ACL IPv6 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > ACL > Avancé > ACL IPv6**.

La page ACL IPv6 s'affiche.

6. Cochez la case associée à la liste de contrôle d'accès IPv6.
7. Dans le champ **ACL IPv6**, spécifiez le nouveau nom.
8. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimer une ACL IPv6

Vous pouvez supprimer un ACL IPv6 avancé dont vous n'avez plus besoin.

Pour supprimer une ACL IPv6 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.
Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.
4. Cliquez sur le bouton **Login** (Connexion).
La page System Information (Informations système) s'affiche.
5. Sélectionnez **sécurité > ACL > Avancé > ACL IPv6**.
La page ACL IPv6 s'affiche.

6. Cochez la case associée à la liste de contrôle d'accès IPv6.
7. Cliquez sur le bouton **Supprimer**.
L'ACL IPv6 est supprimée.
8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurer des règles pour une ACL IPv6 .

Vous pouvez définir des règles pour les ACL IPv6. La définition de liste d'accès comprend des règles qui spécifient si le trafic correspondant aux critères est transféré normalement ou rejeté.

Ajoutez une règle pour une ACL IPv6

Vous pouvez ajouter une règle pour une ACL IPv6.

Pour ajouter une règle pour une ACL IPv6 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.
4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > ACL > Avancé > règles IPv6**.

IPv6 Rules

ACL Name:

IPv6 ACL Rule Table

☐	Sequence Number	Action	Logging	Assign Queue ID	Mirror Interface	Redirect Interface	Match Every	Protocol Type	TCP Flag	Established	Source IPv6 Address	Source IPv6 Prefix Length	Source L4 Port	Destination IPv6 Address	Destination IPv6 Prefix Length
No rules have been configured for this ACL															

S'il n'existe aucune règle, le tableau des règles ACL IPv6 affiche le message *aucune règle n'a été configurée pour cette ACL*. S'il existe une ou plusieurs règles pour la liste de contrôle d'accès, les règles s'affichent dans le tableau des règles de liste de contrôle d'accès IPv6.

6. Dans le menu **nom de l'ACL**, sélectionnez l'ACL IPv6 pour laquelle vous souhaitez ajouter ou modifier une règle.

7. Cliquez sur le bouton **Add** (Ajouter).

La page qui s'affiche vous permet de configurer la règle IPv6.

8. Configurez les options suivantes pour la règle :

- **Numéro de séquence** : Entrez un nombre entier compris entre 1 et 2147483647. Ce numéro est utilisé pour identifier la règle. Une liste de contrôle d'accès IPv6 peut contenir jusqu'à 1023 règles.
- **Action** : Sélectionnez l'action de transfert ACL en sélectionnant l'un des boutons radio suivants :
 - **Permis** : Transférer les paquets qui répondent aux critères de la liste de contrôle d'accès.
 - Refuser Abandonner les paquets qui répondent aux critères de la liste de contrôle d'accès.
- **File d'attente de sortie** : Si vous sélectionnez le bouton radio **autoriser**, sélectionnez l'identificateur de file d'attente de sortie matériel utilisé pour traiter tous les paquets correspondant à cette règle ACL IPv6. La plage d'ID de file d'attente est comprise entre 0 et 6.
- **Enregistrement...** Si vous sélectionnez le bouton radio **refuser**, vous pouvez activer la journalisation pour la liste de contrôle d'accès en sélectionnant le bouton radio **Activer**. (La journalisation dépend de la disponibilité des ressources dans le périphérique.)

Si l'indicateur d'interruption de la liste d'accès est également activé, des interruptions périodiques sont générées, indiquant le nombre de fois que cette règle a été évoquée pendant l'intervalle de rapport. Un intervalle de rapport fixe de cinq minutes est utilisé pour le commutateur. Aucune interruption n'est émise

si le nombre d'occurrences de la règle ACL est égal à zéro pour l'intervalle en cours.

- Interface Si vous sélectionnez le bouton radio **autoriser**, utilisez une interface miroir ou une interface de redirection :
 - Sélectionnez le bouton radio **Mirror interface (interface miroir)** et utilisez le menu pour spécifier l'interface de sortie vers laquelle le flux de trafic correspondant est copié, en plus d'être transféré normalement par l'unité.
 - Sélectionnez le bouton radio **interface de redirection** et utilisez le menu pour spécifier l'interface de sortie vers laquelle le flux de trafic correspondant est forcé, en contournant toute décision de transfert normalement prise par le périphérique.
 - **Correspondre tous les** : Indiquez si tous les paquets doivent correspondre à la règle ACL IPv6 sélectionnée :
 - Désactiver : Tous les paquets ne doivent pas correspondre à la règle ACL IPv6 sélectionnée. Vous pouvez configurer d'autres critères de correspondance sur la page.
 - Activer. Tous les paquets doivent correspondre à la liste de contrôle d'accès et à la règle sélectionnées et sont autorisés ou refusés. Dans ce cas, vous ne pouvez pas configurer d'autres critères de correspondance sur la page.
 - **Type de protocole** : Spécifiez le type de protocole IPv6 de l'une des manières suivantes :
 - Dans le menu **type de protocole**, sélectionnez **IPv6**, **ICMPv6**, **TCP** ou **UDP**.
 - Dans le menu **type de protocole**, sélectionnez **autre** et, dans le champ associé, spécifiez un entier compris entre 0 et 255. Ce numéro représente le protocole IPv6.
 - **Drapeau TCP** : Si vous sélectionnez **TCP** dans le menu **type de protocole**, pour chaque indicateur TCP, vous pouvez spécifier si l'indicateur TCP d'un paquet doit correspondre ou non. Les valeurs des indicateurs TCP sont URG, ACK, PSH, RST, SYN et fin. Vous pouvez définir chaque indicateur TCP séparément sur l'une des options suivantes :
 - Ignorer Le drapeau TCP du paquet est ignoré. Il s'agit de l'option par défaut.
 - Appliquer Un paquet correspond à cette règle ACL si l'indicateur TCP de ce paquet est défini.
 - **Clear** (Effacer) - Un paquet correspond à cette règle ACL si l'indicateur TCP de ce paquet n'est pas défini.
- ❗ **Remarque:** Si les drapeaux RST et ACK sont définis, l'option **Established** est disponible, indiquant qu'une correspondance se produit si les bits spécifiés par RST ou ACK sont définis dans l'en-tête du paquet.

- **SRC** : Dans le champ **SRC**, entrez une adresse IPv6 source ou une plage d'adresses IPv6 source à comparer à l'adresse IPv6 source d'un paquet comme critère de correspondance pour la règle ACL IPv6 sélectionnée :
 - Si vous sélectionnez le bouton radio **adresse IPv6**, entrez une adresse IPv6 ou une plage IPv6 pour appliquer ce critère. Si ce champ est laissé vide, informatique signifie any.
 - Si vous sélectionnez le bouton radio **hôte**, entrez une adresse IPv6 source hôte correspondant à l'adresse IPv6 spécifiée. Si ce champ est laissé vide, informatique signifie any.

L'argument d'adresse IPv6 source doit être sous la forme documentée dans la RFC 2373 où l'adresse est spécifiée en nombres hexadécimaux utilisant des valeurs de 16 bits entre deux-points.

- **SRC L4** : Les options ne sont disponibles que si la sélection dans le menu **type de protocole** est **TCP** ou **UDP**. Utilisez l'option de port L4 source pour spécifier les conditions correspondantes pertinentes pour les numéros de port L4 dans la règle ACL IPv6.

Vous pouvez entrer vous-même le numéro de port ou sélectionner l'un des protocoles suivants dans le menu :

- Les protocoles de port TCP IP source sont **Domain, Echo, FTP, FTP, FTP data, www-http, SMTP, Telnet, POP2, POP3** et **BGP**.
- Les protocoles de port UDP IP source sont **Domain, Echo, SNMP, NTP, RIP, heure, OMS** et **TFTP**.

Chacune de ces valeurs se traduit par son numéro de port équivalent, qui est utilisé à la fois comme début et fin de la plage de ports.

Sélectionnez **autre** dans le menu pour entrer un numéro de port. Si vous sélectionnez autre dans le menu mais laissez le champ vide, informatique signifie tout.

La seule condition correspondante pertinente pour les numéros de port L4 est égale. Cela signifie qu'une règle ACL IPv6 correspond uniquement si le numéro de port source de couche 4 est égal au numéro de port ou au protocole de port spécifié.

- **DST** : Dans le champ **DST**, entrez une adresse IPv6 de destination à comparer à l'adresse IPv6 de destination d'un paquet comme critère de correspondance pour la règle ACL IPv6 sélectionnée :
 - Si vous sélectionnez le bouton radio **adresse IPv6**, entrez une adresse IPv6 pour appliquer ce critère. Si ce champ est laissé vide, informatique signifie any.
 - Si vous sélectionnez le bouton radio **hôte**, entrez une adresse IPv6 source hôte correspondant à l'adresse IPv6 spécifiée. Si ce champ est laissé vide, informatique signifie any.

L'argument d'adresse IPv6 source doit être sous la forme documentée dans la RFC 2373 où l'adresse est spécifiée en nombres hexadécimaux utilisant des valeurs de 16 bits entre deux-points.

- **DST L4** : Les options ne sont disponibles que si la sélection dans le menu **type de protocole** est **TCP** ou **UDP**. Utilisez l'option de port L4 de destination pour spécifier les conditions correspondantes pertinentes pour les numéros de port L4 dans la règle ACL IPv6.

Vous pouvez entrer vous-même le numéro de port ou sélectionner l'un des protocoles suivants dans le menu :

- Les protocoles de port TCP IP de destination sont **domaine**, **Echo**, **FTP**, **données FTP**, **www-http**, **SMTP**, **Telnet**, **POP2**, **POP3** et **BGP**.
- Les protocoles de port UDP IP de destination sont **Domain**, **Echo**, **SNMP**, **NTP**, **RIP**, **heure**, **OMS** et **TFTP**.

Chacune de ces valeurs se traduit par son numéro de port équivalent, qui est utilisé à la fois comme début et fin de la plage de ports.

Sélectionnez **autre** dans le menu pour entrer un numéro de port. Si vous sélectionnez autre dans le menu mais laissez le champ vide, informatique signifie tout.

La seule condition correspondante pertinente pour les numéros de port L4 est égale. Cela signifie qu'une règle ACL IPv6 correspond uniquement si le numéro de port de destination de couche 4 est égal au numéro de port ou au protocole de port spécifié.

- **ICMPv6** : Les champs **type** et **message** sont activés uniquement si le protocole est ICMPv6. Utilisez ces champs pour spécifier une condition de correspondance pour les paquets ICMPv6. Sélectionnez le bouton radio **type** ou **message** :
 - Si vous sélectionnez le bouton radio **type**, notez les points suivants :
 - Les champs **type** et **Code** sont activés uniquement si le protocole est ICMPv6. Utilisez ces champs pour spécifier une condition de correspondance pour les paquets ICMPv6 :
 - Si vous spécifiez des informations dans le champ **type**, la règle ACL IPv6 correspond au type de message ICMPv6 spécifié. La plage de numéros de port peut être comprise entre 0 et 255.
 - Si vous spécifiez des informations dans le champ **Code**, la règle ACL IPv6 correspond au code de message ICMPv6 spécifié. Le code peut être compris entre 0 et 255.
 - Si ces champs sont laissés vides, informatique signifie any.
 - Si vous sélectionnez le bouton radio **message**, notez les points suivants :
 - Sélectionnez le type de message ICMPv6 à faire correspondre à la règle ACL IPv6 sélectionnée. Spécifier un type de message implique que le type

ICMPv6 et le code ICMPv6 sont spécifiés. Le message ICMPv6 est décodé dans le type ICMPv6 correspondant et le code ICMPv6 dans le type ICMP.

- Les types de message ICMPv6 sont **destination-inaccessible**, **écho-réponse**, **écho-requête**, **en-tête**, **saut-limite**, **requête-MLD**, **réduction-MLD**, **rapport-MLD**, **en-tête-suivant**, **no-admin**, **no-route**, **paquet-trop-gros**, **port-inaccessible**, **sollicitation-routeur**, **annonce-routeur**, **renumérotation du routeur**, **inaccessible**, **temps dépassé**, **nd-na** et **nd-ns**.
- fragmentée Sélectionnez le bouton radio **Activer** pour autoriser les fragments initiaux (c'est-à-dire que le bit de fragment est confirmé) ou laissez le bouton radio désactiver par défaut sélectionné pour empêcher l'utilisation des fragments initiaux.

Cette option n'est pas valide pour les règles qui correspondent aux informations L4 telles que le numéro de port TCP, car ces informations sont transportées dans le paquet initial.

- **Étiquette de flux** : Le champ **libellé de flux** est activé uniquement si la sélection dans le menu **type de protocole** est ICMPv6. L'étiquette de flux est un numéro de 20 bits qui est unique à un paquet IPv6 et qui est utilisé par les stations terminales pour indiquer la gestion de la qualité de service dans les routeurs. La plage pour le libellé de flux est comprise entre 0 et 1048575.
- **Service DSCP IPv6** : Spécifiez le champ IP DiffServ Code point (DSCP). Il s'agit d'une configuration facultative.

Le DSCP est défini comme les six bits de poids fort de l'octet de type de service dans l'en-tête IPv6. Entrez un entier compris entre 0 et 63. Pour sélectionner le DSCP IPv6, sélectionnez l'un des mots-clés DSCP. Pour spécifier une valeur numérique, sélectionnez autre et entrez la valeur numérique du DSCP.

- **Limite de débit conforme débit de données** : Spécifiez la valeur du débit de données conforme, qui correspond au débit auquel le trafic de confirmation est limité. La plage est de 1 à 4294967295 secondes.
- **Taille de rafale limite de débit** : Spécifiez la valeur de la taille des rafales, qui correspond à la taille à laquelle les rafales de trafic supérieures au débit de confirmation sont autorisées. La plage est de 1 à 128 secondes.
- Plage de temps Dans le menu **plage horaire**, sélectionnez le planning de minuterie qui doit être associé à la règle. Pour plus d'informations sur les programmations de minuterie, reportez-vous à la section [Programmations de minuterie](#) à la page 247. Si vous n'avez configuré aucun programme de minuterie, le menu ne présente aucune option.

9. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

Le champ État de la règle du tableau indique si la règle est active ou inactive. Vide signifie qu'aucun planning de minuterie n'est associé à la règle.

10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Modifiez les critères de correspondance d'une règle ACL IPv6

Vous pouvez modifier les critères de correspondance d'une règle ACL IPv6.

Pour modifier les critères de correspondance d'une règle ACL IPv6 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > ACL > Avancé > règles IPv6**.

La page règles IPv6 s'affiche.

6. Dans le menu **nom de l'ACL**, sélectionnez l'ACL qui inclut la règle à modifier.

7. Dans le tableau des règles ACL IPv6, cliquez sur la règle.

La règle est un lien hypertexte. La page Configuration de la règle ACL IPv6 s'affiche.

8. Modifiez les critères de la règle ACL IPv6.

9. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimer une règle ACL IPv6

Vous pouvez supprimer une règle ACL IPv6 dont vous n'avez plus besoin.

Pour supprimer une règle ACL IPv6 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > ACL > Avancé > règles IPv6**.

La page règles IPv6 s'affiche.

6. Dans le menu **nom de l'ACL**, sélectionnez l'ACL qui inclut la règle à supprimer.

7. Dans le tableau des règles ACL IPv6, cochez la case associée à la règle.
8. Cliquez sur le bouton **Supprimer**.
La règle est supprimée.
9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurer les liaisons de l'interface ACL IP

.

Lorsque vous liez une liste de contrôle d'accès IPv4 de base, IPv4 étendu ou IPv6 à une interface, toutes les règles que vous avez définies pour la liste de contrôle d'accès IP sont appliquées à l'interface sélectionnée.

Si les ressources du commutateur sont insuffisantes, une tentative de liaison d'une ACL à une interface échoue.

Pour lier une ACL IP à une ou plusieurs interfaces :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.
4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > ACL > Avancé > Configuration de liaison IP**.

L'écran IP Configuration (Configuration IP) s'affiche.

6. Dans le menu **ID ACL**, sélectionnez une ACL IP.

❗ Remarque: La liaison d'une ACL à une interface échoue si le commutateur n'a pas de ressources pour lier une nouvelle ACL. En outre, vous ne pouvez pas lier à la fois une ACL IPv4 et une ACL IPv6 à une interface.

7. Dans le menu **Direction**, sélectionnez la direction de filtrage des paquets pour la liste de contrôle d'accès :

- Trafic entrant La règle s'applique au trafic entrant dans le port.
- **Sortant:** La règle s'applique au trafic sortant du port.

8. Dans le champ **numéro de séquence**, spécifiez éventuellement un numéro pour indiquer l'ordre de la liste d'accès par rapport aux autres listes d'accès déjà affectées à l'interface et à la direction.

Un nombre faible indique un ordre de priorité élevé. Si un numéro de séquence est déjà utilisé pour l'interface et la direction, la liste d'accès spécifiée remplace la liste d'accès actuellement attachée utilisant ce numéro de séquence. Si vous ne spécifiez pas le numéro de séquence (ce qui signifie que la valeur est 0), un numéro de séquence supérieur d'un nombre au numéro de séquence le plus élevé actuellement utilisé pour l'interface et la direction est utilisé. La plage est de 1 à 4294967295.

9. Pour ajouter la liste de contrôle d'accès sélectionnée à un port ou à un lag, dans la table ports (ou, si une pile est configurée, dans l'une des tables ports) ou lag, cliquez sur le port ou le lag pour qu'une coche s'affiche.

Les tables ports et lag affichent les interfaces disponibles pour les liaisons ACL. Vous pouvez ajouter l'ACL à plusieurs ports et LAG.

Les ports du commutateur (unité 1) sont affichés. Si une pile est configurée, les ports de chaque commutateur empilé (unité 1, unité 2, etc.) sont affichés. En outre, tous les LAG sont affichés, qu'une pile soit configurée ou non.

10. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

11. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 185 : Informations sur l'état de liaison de l'interface

Champ	Description
Interface	L'interface sélectionnée.
Direction	Direction de filtrage des paquets sélectionnée pour la liste de contrôle d'accès.
Type de ACL	Type de liste de contrôle d'accès affecté à l'interface et à la direction sélectionnées.
ID/nom ACL	Numéro ou nom de la liste de contrôle d'accès identifiant la liste de contrôle d'accès attribuée à l'interface et à la direction sélectionnées.
Numéro de séquence	Numéro de séquence indiquant l'ordre de la liste de contrôle d'accès spécifiée par rapport aux autres listes de contrôle d'accès affectées à l'interface et à la direction sélectionnées.

Affichez ou supprimez les liaisons IP ACL dans la table de liaison IP ACL .

Vous pouvez afficher ou supprimer des liaisons pour les listes de contrôle d'accès IPv4 de base, IPv4 étendues et IPv6.

Pour afficher ou supprimer des liaisons IP ACL :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **sécurité > ACL > Avancé > table de liaison** .
La page table de liaison IP ACL s'affiche. Le tableau affiche les liaisons IP ACL-interface.
6. Pour supprimer une liaison IP ACL-to-interface, procédez comme suit :
 - a. Cochez la case en regard de l'interface.
 - b. Cliquez sur le bouton **Supprimer**.

La liaison est supprimée.

7. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 186 : Informations sur l'état de liaison de l'interface

Champ	Description
Interface	L'interface sélectionnée.
Direction	Direction de filtrage des paquets sélectionnée pour la liste de contrôle d'accès.
Type de ACL	Type de liste de contrôle d'accès affecté à l'interface et à la direction sélectionnées.
ID/nom ACL	Numéro ou nom de la liste de contrôle d'accès identifiant la liste de contrôle d'accès attribuée à l'interface et à la direction sélectionnées.
Numéro de séquence	Numéro de séquence indiquant l'ordre de la liste de contrôle d'accès spécifiée par rapport aux autres listes de contrôle d'accès affectées à l'interface et à la direction sélectionnées.

Configurer les liaisons ACL VLAN .

Vous pouvez associer une ACL MAC, tout type d'ACL IPv4 ou IPv6 à un VLAN. Lorsque vous le faites, la liste de contrôle d'accès est appliquée à toutes les interfaces qui sont membres du VLAN.

Ajoutez une liaison ACL VLAN

Vous pouvez lier un ID VLAN à une liste de contrôle d'accès et appliquer la direction de filtrage des paquets pour la liste de contrôle d'accès au trafic entrant ou sortant.

Pour ajouter une liaison ACL VLAN :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > ACL > Avancé > table de liaison VLAN**.

La page table de reliure VLAN s'affiche.

6. Dans le champ **VLAN ID**, entrez l'ID VLAN auquel la liaison doit s'appliquer.

7. Dans le menu **Direction**, sélectionnez la direction de filtrage des paquets pour la liste de contrôle d'accès :

- **Trafic entrant** La règle s'applique au trafic entrant dans le port.
- **Sortant**: La règle s'applique au trafic sortant du port.

8. Dans le champ **numéro de séquence**, spécifiez éventuellement un numéro pour indiquer l'ordre de la liste d'accès par rapport aux autres listes d'accès déjà attribuées au VLAN et à la direction.

Un nombre faible indique un ordre de priorité élevé. Si un numéro de séquence est déjà utilisé pour l'ID et la direction VLAN, la liste d'accès spécifiée remplace la liste d'accès actuellement attachée utilisant ce numéro de séquence. Si vous ne spécifiez

pas le numéro de séquence (ce qui signifie que la valeur est 0), un numéro de séquence supérieur d'un nombre au numéro de séquence le plus élevé actuellement utilisé pour l'ID VLAN et la direction est utilisé. La plage est de 1 à 4294967295.

9. Dans le menu **type d'ACL**, sélectionnez le type d'ACL.

Vous pouvez sélectionner une ACL MAC, une ACL IP ou une ACL IPv6.

10. Dans la liste **ID ACL**, sélectionnez l'ID ou le nom de la ACL qui doit être liée à l'VLAN spécifiée.

11. Cliquez sur le bouton **Add** (Ajouter).

La liaison ACL VLAN est ajoutée.

12. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Supprimez une liaison de liste de contrôle d'accès VLAN

Vous pouvez supprimer une liaison entre un ID VLAN et une ACL.

Pour supprimer une liaison ACL VLAN :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > ACL > Avancé > table de liaison VLAN**.

La page table de liaison VLAN s'affiche.

6. Cochez la case correspondant à la liaison VLAN à supprimer.

7. Cliquez sur le bouton **Supprimer**.

La liaison ACL VLAN est supprimée.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

10

Surveillez le commutateur et le réseau

Ce chapitre aborde les sujets suivants :

- Statistiques des ports et des paquets EAP
- Effectuez un test de câble .
- Journaux
- Paramètres hôte du serveur syslog et log
- Journal des interruptions :
- Journaux des événements
- Configurer la journalisation USB
- Port mirroring
- VLAN RSPAN et commutateurs source et de destination
- Surveillance SFlow

Statistiques des ports et des paquets EAP

Vous pouvez afficher les statistiques de port, y compris les statistiques détaillées, et les statistiques de paquets EAP (extensible Authentication Protocol).

Afficher ou effacer les statistiques de port

Vous pouvez afficher un résumé des statistiques de trafic par port sur le commutateur et effacer les statistiques.

Pour afficher ou effacer les statistiques du commutateur :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **surveillance > ports > statistiques des ports** .

La page statistiques PORT s'affiche.

6. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :
 - **1 ou ID d'unité pour un commutateur empilé :**
 - 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
 - **ID d'unité pour un commutateur empilé :** Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
 - LAG Seuls les LAG sont affichés.
 - **Tous:** Les interfaces physiques et les LAG sont affichés, ou pour une pile de commutateurs, les interfaces physiques de tous les commutateurs de la pile et les LAG sont affichés.
7. **Pour configurer une interface unique, cochez la case associée au port ou tapez le numéro de port (par exemple g1) dans le champ aller à l'interface et cliquez sur le bouton aller.**
8. Pour effacer les compteurs, effectuez l'une des opérations suivantes :
 - Pour effacer tous les compteurs de tous les ports du commutateur, cochez la case dans l'en-tête de ligne et cliquez sur le bouton **Effacer**.
 - Pour effacer les compteurs d'un port spécifique, cochez la case correspondant au port et cliquez sur le bouton **Effacer**.
9. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).
10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les statistiques par port affichées sur la page.

Table 187 : Informations statistiques de port

Champ	Description
Interface	L'interface.
Nombre total de paquets reçus sans erreurs	Nombre total de paquets reçus sans erreur.
Paquets reçus avec erreur	Nombre de paquets entrants qui contenaient des erreurs, les empêchant d'être livrés à un protocole de couche supérieure.
Paquets de diffusion reçus	Nombre total de paquets reçus qui ont été dirigés vers l'adresse de diffusion. Cela n'inclut pas les paquets multicast.
Paquets transmis sans erreurs	Nombre de trames transmises par ce port à son segment.
Erreurs de transmission de paquets	Nombre de paquets sortants qui n'ont pas pu être transmis en raison d'erreurs.

Table 187 : Informations statistiques de port (A continué)

Champ	Description
Cadres de collision	Meilleure estimation du nombre total de collisions sur ce segment Ethernet.
Événements liés à la liaison interrompue	Nombre total d'événements de liaison interrompue sur le port.
Lier les volets	Nombre d'occurrences d'événements liaison descendante à liaison montante (c'est-à-dire, un volet de liaison) pendant le temps de rebond.
Débit de réception (Mbit/s)	Débit de données reçu en Mbit/s.
Débit de transmission (Mbit/s)	Débit de données transmis en Mbit/s.
Taux d'erreur reçu	Débit de données reçu avec erreurs en Mbit/s.
Taux d'erreur transmis	Débit de données transmis avec erreurs en Mbps.
Paquets reçus par seconde	Nombre de paquets reçus par seconde.
Paquets transmis par seconde	Nombre de paquets transmis par seconde.
Temps écoulé depuis le dernier effacement des compteurs	Temps écoulé, en jours, heures, minutes et secondes, depuis la dernière effacement des statistiques de ce commutateur.

Afficher ou effacer les statistiques détaillées d'un port

Pour un port spécifique, vous pouvez afficher diverses statistiques de trafic par port ou effacer les statistiques.

Pour afficher et effacer les statistiques détaillées d'un port :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **surveillance > ports > statistiques détaillées des ports**.

La page Port Detailed Statistics s'affiche.

6. Dans le menu **interface**, sélectionnez l'interface (port physique ou lag) pour laquelle vous souhaitez afficher les statistiques.

7. Dans le menu **ID MST**, sélectionnez l>ID MST associé à l'interface (si disponible).

8. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

9. Pour effacer tous les compteurs, cliquez sur le bouton **Effacer**.

Toutes les statistiques du port sont réinitialisées aux valeurs par défaut.

10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les statistiques détaillées des ports affichées sur la page.

Table 188 : Port informations statistiques détaillées

Champ	Description
IfIndex	IfIndex de l'entrée de la table d'interface associée au port.
Type de port	Le port est normal ou l'un des ports suivants : • Miroirs Le port est un port mis en miroir dans une configuration de mise en miroir de ports. • Sonde : Le port est le port de sonde dans une configuration de mise en miroir de ports. • Port Channel : Le port est membre d'un lag.
ID du canal de port	Si le port est membre d'un canal de port, l>ID et le nom de l'interface du canal de port s'affichent. Sinon, désactiver s'affiche.
Rôle du port	Chaque port de pont MST activé se voit attribuer un rôle de port pour chaque Spanning Tree. Le rôle de port est l'une des valeurs suivantes : Racine, désigné, autre, sauvegarde, maître ou Désactivé.

Table 188 : Port informations statistiques détaillées (A continué)

Champ	Description
Mode STP	Mode administratif du protocole Spanning Tree associé au port ou au canal de port. Les options Activer (Spanning Tree est activé (Spanning Tree est activé pour le port) ou désactiver (Spanning Tree est désactivé pour le port).
État STP	État Spanning Tree actuel du port. Cet état contrôle l'action qu'un port effectue à la réception d'une trame. Si le port détecte un port défectueux, informatique place ce port dans l'état cassé. Les états sont définis dans IEEE 802.1D : • Désactivé(e) • Bloquée • Ecoute • Formation • Suivant • Cassé
Mode Admin	État de l'administration du contrôle portuaire. Le port doit être activé pour que informatique puisse entrer dans le réseau. La valeur par défaut est Activer.
Mode de contrôle du débit	Indique si le contrôle de flux est activé ou désactivé pour le port. Ce champ ne s'applique pas aux LAG.
Mode LACP	État administratif du protocole de contrôle de l'agrégation de liens. Le mode doit être activé pour que le port participe à l'agrégation de liens.
Mode physique	La vitesse du port et le mode duplex. En mode de négociation automatique, le mode duplex et la vitesse sont définis par le processus de négociation automatique.
État physique	La vitesse du port et le mode duplex.
Etat de liaison	Indique si la liaison est active ou inactive.
Lien Trap	Indique si le port envoie une interruption lorsque l'état de la liaison change.
Paquets RX et TX 64 octets	Le nombre total de paquets (y compris les paquets défectueux) reçus ou transmis d'une longueur de 64 octets (à l'exclusion des bits de trame mais incluant les octets FCS).
Paquets RX et TX 65-127 octets	Le nombre total de paquets (y compris les paquets défectueux) reçus ou transmis dont la longueur était comprise entre 65 et 127 octets inclus (à l'exclusion des bits de trame mais incluant les octets FCS).
Paquets RX et TX 128-255 octets	Le nombre total de paquets (y compris les paquets défectueux) reçus ou transmis dont la longueur était comprise entre 128 et 255 octets inclus (à l'exclusion des bits de trame mais incluant les octets FCS).
Paquets RX et TX 256-511 octets	Le nombre total de paquets (y compris les paquets défectueux) reçus ou transmis dont la longueur était comprise entre 256 et 511 octets inclus (à l'exclusion des bits de trame mais incluant les octets FCS).

Table 188 : Port informations statistiques détaillées (A continué)

Champ	Description
Paquets RX et TX 512-1023 octets	Le nombre total de paquets (y compris les paquets défectueux) reçus ou transmis dont la longueur était comprise entre 512 et 1023 octets inclus (à l'exclusion des bits de trame mais incluant les octets FCS).
Paquets RX et TX 1024-1518 octets	Le nombre total de paquets (y compris les paquets défectueux) reçus ou transmis dont la longueur était comprise entre 1024 et 1518 octets inclus (à l'exclusion des bits de trame mais incluant les octets FCS).
Paquets RX et TX 1519-2047 octets	Le nombre total de paquets (y compris les paquets défectueux) reçus ou transmis dont la longueur était comprise entre 1519 et 2047 octets inclus (à l'exclusion des bits de trame mais incluant les octets FCS).
Paquets RX et TX 2048-4095 octets	Le nombre total de paquets (y compris les paquets défectueux) reçus ou transmis dont la longueur était comprise entre 2048 et 4095 octets inclus (à l'exclusion des bits de trame mais incluant les octets FCS).
Paquets RX et TX 4096-9216 octets	Le nombre total de paquets (y compris les paquets défectueux) reçus ou transmis dont la longueur était comprise entre 4096 et 9216 octets inclus (à l'exclusion des bits de trame mais incluant les octets FCS).
Octets reçus	Nombre total d'octets de données (y compris ceux contenus dans des paquets erronés) reçus sur le réseau (à l'exclusion des bits de trame mais y compris les octets FCS). Cet objet peut être utilisé comme une estimation raisonnable de l'utilisation d'Ethernet. Si une plus grande précision est souhaitée, les objets etherStatsPkts et etherStatsOctets doivent être échantillonnés avant et après un intervalle commun.
Paquets reçus 64 octets	Le nombre total de paquets (y compris les paquets défectueux) reçus d'une longueur de 64 octets (à l'exclusion des bits de trame mais en incluant les octets FCS).
Paquets reçus 65-127 octets	Nombre total de paquets (y compris les paquets défectueux) reçus dont la longueur était comprise entre 65 et 127 octets inclus (à l'exclusion des bits de trame mais incluant les octets FCS).
Paquets reçus 128-255 octets	Nombre total de paquets (y compris les paquets défectueux) reçus dont la longueur était comprise entre 128 et 255 octets inclus (à l'exclusion des bits de trame mais incluant les octets FCS).
Paquets reçus 256-511 octets	Nombre total de paquets (y compris les paquets défectueux) reçus dont la longueur était comprise entre 256 et 511 octets inclus (à l'exclusion des bits de trame mais incluant les octets FCS).
Paquets reçus 512-1023 octets	Nombre total de paquets (y compris les paquets défectueux) reçus dont la longueur était comprise entre 512 et 1023 octets inclus (à l'exclusion des bits de trame mais incluant les octets FCS).
Paquets reçus 1024-1518 octets	Nombre total de paquets (y compris les paquets défectueux) reçus dont la longueur était comprise entre 1024 et 1518 octets inclus (à l'exclusion des bits de trame mais incluant les octets FCS).
Paquets reçus > 1518 octets	Nombre total de paquets reçus qui étaient plus longs que 1518 octets (à l'exclusion des bits de trame, mais incluant les octets FCS) et qui étaient autrement bien formés.

Table 188 : Port informations statistiques détaillées (A continué)

Champ	Description
Nombre total de paquets reçus sans erreurs	Nombre total de paquets reçus sans erreur.
Paquets unicast reçus	Nombre de paquets unicast de sous-réseau livrés à un protocole de couche supérieure.
Paquets multidiffusion reçus	Nombre total de paquets reçus qui ont été dirigés vers une adresse de multidiffusion. Ce nombre n'inclut pas les paquets dirigés vers l'adresse de diffusion.
Paquets de diffusion reçus	Nombre total de paquets reçus qui ont été dirigés vers l'adresse de diffusion. Cela n'inclut pas les paquets multicast.
Réception des paquets ignorés	Nombre de paquets entrants qui ont été rejetés même si aucune erreur n'a été détectée qui empêcherait les paquets d'être livrés à un protocole de couche supérieure. Une raison possible pour rejeter un paquet peut être de libérer de l'espace tampon.
Nombre total de paquets reçus avec des erreurs MAC	Nombre total de paquets entrants qui contenaient des erreurs les empêchant d'être distribués à un protocole de couche supérieure.
Jabbers reçu	Nombre total de paquets reçus de plus de 1518 octets (à l'exclusion des bits de tramage, mais incluant les octets FCS), et ayant soit une mauvaise séquence de contrôle de trame (FCS) avec un nombre entier d'octets (erreur FCS), soit une mauvaise FCS avec un nombre non entier d'octets (erreur d'alignement). Cette définition de Jabber est différente de la définition de IEEE-802,3 section 8.2.1.5 (10BASE5) et section 10.3.1.4 (10BASE2). Ces documents définissent Jabber comme la condition dans laquelle un paquet dépasse 20 ms. La plage autorisée pour détecter Jabber est comprise entre 20 ms et 150 ms.
Fragments reçus	Nombre total de paquets reçus dont la longueur était inférieure à 64 octets avec CRC D'ERREUR (à l'exclusion des bits de trame mais incluant les octets FCS).
Reçu sous-dimensionné	Nombre total de paquets reçus d'une longueur inférieure à 64 octets avec un BON CRC (à l'exclusion des bits de trame mais incluant les octets FCS).
Erreurs d'alignement	Nombre total de paquets reçus avec une longueur (à l'exclusion des bits de trame, mais incluant les octets FCS) comprise entre 64 et 1518 octets, inclus, mais avec une mauvaise séquence de contrôle de trame (FCS) avec un nombre non entier d'octets.
Erreurs Rx FCS	Nombre total de paquets reçus avec une longueur (à l'exclusion des bits de trame, mais incluant les octets FCS) comprise entre 64 et 1518 octets inclus, mais avec une séquence de contrôle de trame erronée (FCS) avec un nombre entier d'octets
Dépassements	Nombre total de trames rejetées car ce port était surchargé de paquets entrants et n'a pas pu suivre le flux entrant.
Nombre total de paquets reçus non transférés	Nombre de trames valides reçues qui ont été rejetées (c'est-à-dire filtrées) par le processus de transfert.

Table 188 : Port informations statistiques détaillées (A continué)

Champ	Description
Trames de pause 802.3x reçues	Nombre de trames de contrôle MAC reçues sur cette interface avec un opcode indiquant l'opération PAUSE. Ce compteur n'augmente pas lorsque l'interface fonctionne en mode semi-duplex.
Type de trame inacceptable	Nombre de trames rejetées de ce port en raison d'un type de trame inacceptable.
Nombre total de paquets transmis (octets)	Nombre total d'octets de données (y compris ceux contenus dans des paquets erronés) transmis sur le réseau (à l'exclusion des bits de trame mais y compris les octets FCS). Cet objet peut être utilisé comme une estimation raisonnable de l'utilisation d'Ethernet. Si une plus grande précision est souhaitée, les objets etherStatsPkts et etherStatsOctets doivent être échantillonnés avant et après un intervalle commun.
Paquets transmis 64 octets	Le nombre total de paquets (y compris les paquets défectueux) reçus d'une longueur de 64 octets (à l'exclusion des bits de trame mais en incluant les octets FCS).
Paquets transmis 65-127 octets	Nombre total de paquets (y compris les paquets défectueux) reçus dont la longueur était comprise entre 65 et 127 octets inclus (à l'exclusion des bits de trame mais incluant les octets FCS).
Paquets transmis 128-255 octets	Nombre total de paquets (y compris les paquets défectueux) reçus dont la longueur était comprise entre 128 et 255 octets inclus (à l'exclusion des bits de trame mais incluant les octets FCS).
Paquets transmis 256-511 octets	Nombre total de paquets (y compris les paquets défectueux) reçus dont la longueur était comprise entre 256 et 511 octets inclus (à l'exclusion des bits de trame mais incluant les octets FCS).
Paquets transmis 512-1023 octets	Nombre total de paquets (y compris les paquets défectueux) reçus dont la longueur était comprise entre 512 et 1023 octets inclus (à l'exclusion des bits de trame mais incluant les octets FCS).
Paquets transmis 1024-1518 octets	Nombre total de paquets (y compris les paquets défectueux) reçus dont la longueur était comprise entre 1024 et 1518 octets inclus (à l'exclusion des bits de trame mais incluant les octets FCS).
Paquets transmis > 1518 octets	Nombre total de paquets transmis qui étaient plus longs que 1518 octets (à l'exclusion des bits de trame, mais incluant les octets FCS) et qui étaient autrement bien formés. Ce compteur a un taux d'incrément maximum de 815 comptes par seconde à 10 Mo/s.
Taille maximale du cadre	La taille de trame est la taille de trame Ethernet maximale que l'interface prend en charge ou est configurée pour utiliser, y compris l'en-tête Ethernet, le CRC et la charge utile. La taille minimale est de 1500 ; la taille maximale est de 12270 ; la taille par défaut est de 9198.
Nombre total de paquets transmis	Nombre de trames transmises au segment du port.
Paquets unicast transmis	Nombre total de paquets que les protocoles de niveau supérieur ont demandés et qui sont transmis à une adresse de monodiffusion de sous-réseau, y compris ceux qui ont été rejetés ou non envoyés.

Table 188 : Port informations statistiques détaillées (A continué)

Champ	Description
Paquets multicast transmis	Nombre total de paquets que les protocoles de niveau supérieur ont demandés et qui sont transmis à une adresse de multidiffusion, y compris ceux qui ont été rejetés ou qui n'ont pas été envoyés.
Paquets de diffusion transmis	Nombre total de paquets que les protocoles de niveau supérieur ont demandés et qui sont transmis à l'adresse de diffusion, y compris ceux qui ont été rejetés ou qui n'ont pas été envoyés.
Paquets de transmission ignorés	Nombre total de paquets sortants qui ont été rejetés même si aucune erreur n'a été détectée qui empêcherait les paquets d'être livrés à un protocole de couche supérieure. Une raison possible pour rejeter un paquet peut être de libérer de l'espace tampon.
Nombre total d'erreurs de transmission	Somme des collisions simples, multiples et excessives.
Erreurs FCS TX	Nombre total de paquets transmis d'une longueur (à l'exclusion des bits de trame mais incluant les octets FCS) comprise entre 64 et 1518 octets inclus, et d'une séquence de contrôle de trame (FCS) incorrecte avec un nombre entier d'octets.
Nombre total de paquets de transmission ignorés	Somme des trames de collision uniques rejetées, des trames de collision multiples rejetées et des trames excessives rejetées.
Cadres de collision simples	Nombre de trames transmises avec succès sur une interface particulière pour lesquelles la transmission est inhibée par exactement une collision.
Cadres de collision multiples	Nombre de trames transmises avec succès sur une interface particulière pour lesquelles la transmission est inhibée par plusieurs collisions.
Cadres de collision excessifs	Nombre de trames pour lesquelles la transmission sur une interface particulière échoue en raison de collisions excessives.
BPDU STP reçues	Nombre de BPDU STP reçues.
BPDU STP transmises	Nombre de BPDU STP transmises.
BPDU RSTP reçues	Nombre de BPDU RSTP reçues.
BPDU RSTP transmises	Nombre de BPDU RSTP transmises.
BPDU MSTP reçues	Nombre de BPDU MSTP reçues.
BPDU MSTP transmises	Nombre de BPDU MSTP transmises.
Trames de pause 802.3x transmises	Nombre de trames de contrôle MAC transmises avec un opcode indiquant l'opération PAUSE. Ce compteur n'augmente pas lorsque l'interface fonctionne en mode semi-duplex.
PDU GVRP reçues	Nombre de PDU GVRP reçues dans la couche GARP.
PDU GVRP transmises	Nombre de PDU GVRP transmises depuis la couche GARP.

Table 188 : Port informations statistiques détaillées (A continué)

Champ	Description
Échec des enregistrements GVRP	Nombre de tentatives d'enregistrement GVRP impossible.
PDU GMRP reçues	Nombre de PDU GMRP reçues de la couche GARP.
PDU GMRP transmises	Nombre de PDU GMRP transmises depuis la couche GARP.
Échec des enregistrements GMRP	Nombre de tentatives d'enregistrement GMRP impossible.
Trames EAPOL reçues	Nombre de trames EAPOL valides de tout type reçues par cet authentificateur.
Trames EAPOL transmises	Nombre de trames EAPOL de tout type qui ont été transmises par cet authentificateur.
Intervalle de chargement	Période en secondes pendant laquelle les données sont utilisées pour calculer les statistiques de charge.
Débit de réception (Mbit/s)	Débit de données reçu en Mbit/s.
Débit de transmission (Mbit/s)	Débit de données transmis en Mbit/s.
Taux d'erreur reçu	Débit de données reçu avec erreurs en Mbit/s.
Taux d'erreur transmis	Débit de données transmis avec erreurs en Mbps.
Paquets reçus par seconde	Nombre de paquets reçus par seconde.
Paquets transmis par seconde	Nombre de paquets transmis par seconde.
Pourcentage d'utilisation reçu	Utilisation du trafic reçu, arrondie au pourcentage entier le plus proche.
Pourcentage d'utilisation transmis	Utilisation du trafic transmis, arrondie au pourcentage entier le plus proche.
Temps écoulé depuis le dernier effacement des compteurs	Temps écoulé, en jours, heures, minutes et secondes, depuis la dernière effacement des statistiques de ce commutateur.

Afficher ou effacer les statistiques EAP et EAPOL .

Vous pouvez afficher des informations sur les paquets EAP (extensible Authentication Protocol) et EAP over LAN (EAPOL) reçus sur les ports physiques.

Pour afficher ou effacer les statistiques EAP et EAPOL :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.
4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **surveillance > ports > statistiques EAP** .
La page statistiques EAP s'affiche.
6. Si une pile est configurée, indiquez si vous souhaitez afficher les interfaces physiques d'un commutateur ou de tous les commutateurs de la pile :
 - **ID d'unité pour un commutateur empilé** : Les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
Si aucune pile de commutateurs n'est configurée, la seule option est l'ID d'unité 1.
 - **Tous** : Les interfaces physiques de tous les commutateurs de la pile sont affichées.
Si aucune pile de commutateurs n'est configurée, l'option tous n'a aucun effet.
7. Pour effacer les compteurs, ce qui réinitialise les statistiques EAP et EAPOL aux valeurs par défaut, effectuez l'une des opérations suivantes :

- Pour effacer les compteurs d'un port spécifique, cochez la case associée au port, puis cliquez sur le bouton **Effacer**.
- Pour effacer les compteurs de plusieurs ports, cochez les cases associées aux ports, puis cliquez sur le bouton **Effacer**.
- Pour effacer tous les compteurs de tous les ports, cochez la case dans l'en-tête de ligne, puis cliquez sur le bouton **Effacer**.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

9. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).

Le tableau suivant décrit les statistiques EAP affichées sur la page.

Table 189 : Informations statistiques EAP

Champ	Description
Port	Numéro de port.
Fonctionnalités de consultation	Les capacités PAE du port.
Trames EAPOL reçues	Nombre de trames EAPOL valides de tout type reçues par cet authentificateur.
Trames EAPOL transmises	Nombre de trames EAPOL de tout type qui ont été transmises par cet authentificateur.
Trames de début EAPOL reçues	Nombre de trames de début EAPOL reçues par cet authentificateur.
Trames de déconnexion EAPOL reçues	Nombre de trames de déconnexion EAPOL reçues par cet authentificateur.
Version de la dernière trame EAPOL	Numéro de version du protocole transporté dans la trame EAPOL la plus récente reçue.
Source de la dernière trame EAPOL	Adresse MAC source transportée dans la dernière trame EAPOL reçue.
Trames EAPOL non valides reçues	Nombre de trames EAPOL reçues par cet authentificateur dans lesquelles le type de trame n'est pas reconnu.
Trames d'erreur de longueur EAPOL reçues	Nombre de trames EAPOL reçues par cet authentificateur dans lesquelles le type de trame n'est pas reconnu.
Réponse EAP/trames ID reçues	Nombre de trames réponse/identité EAP reçues par cet authentificateur.
Trames de réponse EAP reçues	Nombre de trames de réponse EAP valides (autres que les trames resp./ID) reçues par cet authentificateur.
Demandes EAP/trames ID transmises	Nombre de trames d'identité/requête EAP transmises par cet authentificateur.
Trames de requête EAP transmises	Nombre de trames de requête EAP (autres que les trames de requête/identité) transmises par cet authentificateur.

Effectuez un test de câble .

Vous pouvez tester et afficher des informations sur les câbles connectés aux ports du commutateur.

Pour effectuer un test de câble :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **surveillance > ports > test de câble** .

La page test de câble s'affiche.

6. Si une pile est configurée, indiquez si vous souhaitez afficher les interfaces physiques d'un commutateur ou de tous les commutateurs de la pile :

- **ID d'unité pour un commutateur empilé** : Les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.

Si aucune pile de commutateurs n'est configurée, la seule option est l'ID d'unité 1.

- **Tous** : Les interfaces physiques de tous les commutateurs de la pile sont affichées.

Si aucune pile de commutateurs n'est configurée, l'option tous n'a aucun effet.

7. Cochez les cases associées aux ports physiques pour lesquels vous souhaitez tester les câbles.

8. Cliquez sur le bouton **Apply** (Appliquer).

Un test de câble est effectué sur l'interface sélectionnée. Le test de câble peut prendre jusqu'à deux secondes. Si le port a une liaison active, l'état du câble est toujours normal. La commande renvoie une estimation de longueur de câble si cette fonction est prise en charge par le PHY pour la vitesse de liaison actuelle. Notez que si la liaison est interrompue et qu'un câble est connecté à un adaptateur Ethernet 10/100, l'état du câble peut être ouvert ou court-circuité car certains adaptateurs Ethernet laissent les paires de fils inutilisées non terminées ou mises à la terre.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 190 : Test de câble

Champ	Description
État du câble	Indique l'état du câble : • Normal. Le câble fonctionne correctement. • Ouvrir. Le câble est débranché ou un connecteur défectueux existe. • Court-circuit : Il existe un court-circuit électrique dans le câble. • Echec du test de câble : Impossible de déterminer l'état du câble. Le câble fonctionne peut-être. • Non vérifié Le câble n'est pas encore testé. • Type de câble non valide : Le type de câble n'est pas pris en charge.
Longueur de câble	Longueur estimée du câble en mètres. La longueur est affichée sous la forme d'une plage comprise entre la longueur estimée la plus courte et la longueur estimée la plus longue. Inconnu s'affiche si la longueur du câble n'a pas pu être déterminée. La longueur du câble est affichée uniquement si l'état du câble est normal.
Emplacement de la défaillance	Distance estimée en mètres entre l'extrémité du câble et l'emplacement de la défaillance. L'emplacement de la défaillance s'affiche uniquement si l'état du câble est ouvert ou court-circuité.

Journaux

Le commutateur génère des messages en réponse à des événements, des défaillances et des erreurs ainsi qu'à des changements de configuration ou à d'autres événements. Ces messages sont stockés localement et peuvent être transférés à un ou plusieurs points de collecte centralisés à des fins de surveillance ou de stockage d'archives à long terme (voir [Paramètres hôte du serveur syslog et log](#) à la page 1109). La configuration

locale et distante de la capacité d'enregistrement comprend le filtrage des messages enregistrés ou transmis en fonction de la gravité et du composant générateur.

Gérer et afficher le journal de mémoire

Le journal de mémoire stocke les messages en mémoire en fonction des paramètres du composant de message et de la gravité. Vous pouvez définir l'état administratif et le comportement des journaux dans la mémoire tampon du système. Ces messages de journal sont effacés lorsque le commutateur redémarre.

Pour gérer et afficher le journal de mémoire :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **surveillance > journaux > Journal mémoire**.

La page Journal mémoire s'affiche.

6. Sélectionnez l'un des boutons radio Statut administrateur suivants :

- Activer. Activez le commutateur pour consigner les messages par défaut. Il s'agit de l'option par défaut.
 - Désactiver : Empêcher le commutateur de consigner les messages par défaut.
7. Dans le menu **comportement**, spécifiez le comportement du journal lorsque informatique est plein :
- **Liage** : Lorsque la mémoire tampon est pleine, les messages de journal les plus anciens sont supprimés lorsque le système enregistre les nouveaux messages.
 - **Arrêt sur Full** : Lorsque la mémoire tampon est pleine, le système arrête de consigner les nouveaux messages et conserve tous les messages de journal existants.
8. Dans le menu **filtre de gravité**, sélectionnez le niveau de consignation des messages à consigner.

Les messages de journal avec le niveau de gravité sélectionné et tous les messages de journal de gravité supérieure sont consignés. Par exemple, si vous sélectionnez **avertissement**, les messages consignés incluent avertissement, erreur, critique, alerte et urgence. Le niveau de gravité par défaut est informatif (6).

La gravité peut être l'un des niveaux suivants :

- Urgence Niveau 0, le niveau d'avertissement le plus élevé. Si le périphérique est en panne ou ne fonctionne pas correctement, un journal d'urgence est enregistré sur le périphérique.
- Avertir Niveau 1, le deuxième niveau d'avertissement le plus élevé. Un journal d'alertes est enregistré en cas de dysfonctionnement grave de l'appareil, par exemple en cas de panne de toutes les fonctions de l'appareil.
- **Critique**. Niveau 2, le troisième niveau d'avertissement le plus élevé. Un journal critique est enregistré en cas de dysfonctionnement critique d'un périphérique, par exemple lorsque deux ports de périphérique ne fonctionnent pas, tandis que les autres ports de périphérique restent fonctionnels.
- Erreur : Niveau 3, une erreur de périphérique s'est produite, par exemple un port étant hors ligne.
- **Avertissement** : Niveau 4, le niveau le plus bas d'un avertissement de périphérique.
- Avis : Niveau 5, fournit aux administrateurs réseau des informations sur le périphérique.
- **Information** : Niveau 6, fournit des informations sur le périphérique. Il s'agit de l'option par défaut.
- Débogage Niveau 7, fournit des informations détaillées sur le journal.

❗ Remarque: Un journal enregistre les messages égaux ou supérieurs à un seuil de gravité configuré.

9. Dans le champ **seuil**, entrez le pourcentage d'espace journal qui, s'il est dépassé, provoque l'arrêt de la journalisation.

Entrez un pourcentage compris entre 1 et 100. Le numéro par défaut est 80.

Le seuil s'applique uniquement si la sélection dans le menu **comportement** est **Stop-on-Full**. Par défaut, la sélection par défaut dans le menu **comportement** est **boucle** et le seuil ne s'applique pas.

10. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

Le tableau Journal de la mémoire s'affiche sur la page Journal de la mémoire.

Le champ nombre total de messages affiche le nombre de messages enregistrés par le système en mémoire. Par défaut, jusqu'à 160 entrées (80 % du maximum de 200) parmi les entrées les plus récentes peuvent être affichées sur la page.

Le reste de la page affiche les messages du journal mémoire. Le format du message de journal est le même pour les messages affichés pour le journal des messages, le journal permanent ou le journal de console. Les messages consignés sur un collecteur ou un relais via syslog prennent également en charge le même format.

L'exemple suivant illustre le format standard d'un message de journal :

```
<189> Jun 21 2024 00:00:18: AAA-5-CONNECT: New http connection  
for user admin, source 192.168.1.111 ACCEPTED
```

Le message a été généré comme gravité 189 (avis, niveau 5) le 21 juin 2024 à 00:00:18 par le composant AAA. Le message indique que l'administrateur a réussi à se connecter à l'interface de gestion HTTP à partir d'un hôte dont l'adresse IP est 192.168.1.111.

Le numéro de gravité dans le message est généré par une combinaison de l'établissement et de la gravité. Dans l'exemple précédent, la fonction par défaut 23 est multipliée par 8 et la gravité (5) est ajoutée : 23 8 5 189

11. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).
12. Pour effacer les entrées du journal, cliquez sur le bouton **Clear Log** (Effacer le journal).
13. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Format du journal des messages

Cette rubrique s'applique au format de tous les messages consignés affichés pour le journal des messages, le journal permanent ou le journal de la console.

Les messages consignés dans un collecteur ou un relais via syslog utilisent un format identique :

- <15>Aug 24 05 :34 :05 0,0.0.0-1 MSTP[2110] : mspt_api.c(318) 237%% interface 12 est passé à l'état root à l'expiration du délai d'expiration de l'âge du message.
Cet exemple indique un message de gravité 7 (15 mod 8) (debug) sur un commutateur et généré par le composant MSTP exécuté dans l'ID de thread 2110 le 24 août 05 :34 :05 par la ligne 318 du fichier mspt_api.c. Il s'agit du 237e message enregistré avec l'IP système 0.0.0.0 et l'ID de tâche 1.
- <15>Aug 24 05 :34 :05 STK0 MSTP[2110] : mspt_api.c(318) 237%% interface 12 est passé à l'état root à l'expiration du délai d'expiration de l'âge du message.
Cet exemple indique un message de niveau utilisateur (1) avec un niveau de gravité 7 (débogage) sur un système qui n'est pas un commutateur et généré par le composant MSTP exécuté dans l'ID de thread 2110 le 24 août 05 :34 :05 par la ligne 318 du fichier mspt_api.c. Il s'agit du 237e message enregistré. Les messages consignés dans un collecteur ou un relais via syslog utilisent un format identique au message précédent.
- Nombre total de messages : Pour le journal des messages, seules les 200 dernières entrées sont affichées sur la page.

Active ou désactive le journal de configuration des commandes

Le commutateur peut consigner les modifications apportées à l'aide des commandes de configuration CLI.

Pour activer ou désactiver le journal de configuration des commandes :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **Monitoring > Logs > Command Log Configuration**.

La page Configuration du journal des commandes s'affiche.

6. Sélectionnez l'un des boutons radio Statut administrateur suivants :

- Activer. Activez le commutateur pour consigner les commandes de configuration CLI. Il s'agit de l'option par défaut.
- Désactiver : Empêchez le commutateur de consigner les commandes de configuration CLI.

7. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Activer ou désactiver la journalisation de la console

Le commutateur peut consigner des messages sur un périphérique série connecté au commutateur.

Pour activer ou désactiver la journalisation de la console :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **surveillance > journaux > Configuration du journal de la console** .

La page Configuration du journal de la console s'affiche.

6. Sélectionnez l'un des boutons radio Statut administrateur suivants :

- Activer. Activez le commutateur pour consigner les messages sur un périphérique série. Il s'agit de l'option par défaut.
- Désactiver : Empêchez le commutateur de consigner des messages sur un périphérique série.

7. Dans le menu **filtre de gravité**, sélectionnez le niveau de consignation des messages à consigner.

Les messages de journal avec le niveau de gravité sélectionné et tous les messages de journal de gravité supérieure sont consignés. Par exemple, si vous sélectionnez **avertissement**, les messages consignés incluent avertissement, erreur, critique, alerte et urgence. Le niveau de gravité par défaut est Error (erreur) (3).

La gravité peut être l'un des niveaux suivants :

- Urgence Niveau 0, le niveau d'avertissement le plus élevé. Si le périphérique est en panne ou ne fonctionne pas correctement, un journal d'urgence est enregistré sur le périphérique.
- Avertir Niveau 1, le deuxième niveau d'avertissement le plus élevé. Un journal d'alertes est enregistré en cas de dysfonctionnement grave de l'appareil, par exemple en cas de panne de toutes les fonctions de l'appareil.

- **Critique.** Niveau 2, le troisième niveau d'avertissement le plus élevé. Un journal critique est enregistré en cas de dysfonctionnement critique d'un périphérique, par exemple lorsque deux ports de périphérique ne fonctionnent pas, tandis que les autres ports de périphérique restent fonctionnels.
- Erreur : Niveau 3, une erreur de périphérique s'est produite, par exemple un port étant hors ligne. Il s'agit de l'option par défaut.
- **Avertissement** : Niveau 4, le niveau le plus bas d'un avertissement de périphérique.
- Avis : Niveau 5, fournit aux administrateurs réseau des informations sur le périphérique.
- **Information** : Niveau 6, fournit des informations sur le périphérique.
- Débogage Niveau 7, fournit des informations détaillées sur le journal.

❗ **Remarque:** Un journal enregistre les messages égaux ou supérieurs à un seuil de gravité configuré.

8. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Paramètres hôte du serveur syslog et log

Vous pouvez laisser le commutateur envoyer des messages de journal à un ou plusieurs serveurs, c'est-à-dire à des hôtes de journalisation distants. Un serveur de journaux distant est identique à un hôte syslog distant.

Vous devez activer le journal du serveur sur le commutateur et spécifier un ou plusieurs hôtes syslog distants.

Configurez les paramètres syslog

Pour configurer les paramètres syslog :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **surveillance > journaux > Journal du serveur**.

La page Journal du serveur s'affiche.

6. Sélectionnez l'un des boutons radio Statut administrateur suivants :
 - Activer. Le commutateur envoie des messages de journal à tous les serveurs syslog configurés.
 - Désactiver : Le commutateur cesse d'envoyer des messages de journal à tous les serveurs syslog configurés.
7. Dans le champ **Port UDP local**, spécifiez le numéro de port que le commutateur utilise pour envoyer les messages de journal aux serveurs syslog.

La plage est de 1 à 65535. Le port par défaut est 514.

8. Dans le menu **interface source**, sélectionnez l'interface source ou l'VLAN à utiliser pour la communication syslog. Par défaut, les options suivantes s'affichent dans le menu :

- **Aucun** : L'adresse IP principale de l'interface d'origine (sortante) est utilisée comme adresse source.
- **VLAN 1** : L'adresse IP principale de VLAN 1 est utilisée comme adresse source. Il s'agit de la sélection par défaut.
- **Port de service** : L'adresse IP du port de gestion est utilisée comme adresse source.

Selon la configuration de votre commutateur, les options suivantes peuvent s'afficher :

- **Un autre identifiant VLAN** : L'adresse IP principale d'un VLAN autre que VLAN 1 est utilisée comme adresse source.
- **Interface de routage** : L'adresse IP principale d'une interface de routage est utilisée comme adresse source.
- **VLAN de routage** : L'adresse IP principale d'une interface de routage VLAN est utilisée comme adresse source.
- **Interface de bouclage de routage** : L'adresse IP principale d'une interface de bouclage de routage est utilisée comme adresse source.
- **Différent** : Pour certaines fonctionnalités, *différents* peuvent s'afficher. Cela signifie que l'interface source est configurée séparément.

❗ **Remarque** : La fonction syslog du commutateur peut enregistrer les messages de journal simultanément sur un serveur distant et sur un périphérique de stockage USB.

9. Pour enregistrer simultanément les messages du journal sur un périphérique de stockage USB, dans le champ **nom du fichier USB**, spécifiez le nom du fichier USB.

Le nom de fichier ne peut pas inclure les symboles suivants : V : * ? " < > !. Vous pouvez saisir jusqu'à 64 caractères. Les 64 caractères sont uniquement la longueur du nom de fichier, l'extension est automatiquement ajoutée.

10. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

11. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 191 : Informations de configuration syslog

Champ	Description
Messages reçus	Nombre de messages reçus par le processus de journal. Cela inclut les messages qui sont supprimés ou ignorés.
Messages relayés	Nombre de messages syslog relayés.
Messages ignorés	Nombre de messages syslog ignorés.

Ajoutez un serveur syslog

Pour ajouter un serveur syslog :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **surveillance > journaux > Journal du serveur** .

La page Journal du serveur s'affiche.

6. Dans le tableau Configuration du serveur, configurez les paramètres suivants :

- **Type d'adresse IP** : Spécifiez le type d'adresse IP du serveur syslog, qui peut être **IPv4**, **IPv6** ou **DNS**.
- **Adresse hôte** : Spécifiez l'adresse IP ou le nom d'hôte du serveur syslog.
- **Port**. Spécifiez le port sur le serveur syslog. Le numéro de port par défaut est 514.
- **Filtre de gravité** : Utilisez le menu pour sélectionner la gravité des journaux qui doivent être envoyés au serveur syslog. Les journaux avec le niveau de gravité sélectionné et tous les journaux de gravité supérieure sont envoyés à l'hôte. Par

exemple, si vous sélectionnez **erreur**, les messages consignés incluent erreur, critique, alerte et urgence. La gravité peut être l'un des niveaux suivants :

- Urgence Niveau 0, le niveau d'avertissement le plus élevé. Si le périphérique est en panne ou ne fonctionne pas correctement, un journal d'urgence est enregistré sur le périphérique.
- Avertir Niveau 1, le deuxième niveau d'avertissement le plus élevé. Un journal d'alertes est enregistré en cas de dysfonctionnement grave de l'appareil, par exemple en cas de panne de toutes les fonctions de l'appareil.
- **Critique**. Niveau 2, le troisième niveau d'avertissement le plus élevé. Un journal critique est enregistré en cas de dysfonctionnement critique d'un périphérique, par exemple lorsque deux ports de périphérique ne fonctionnent pas, tandis que les autres ports de périphérique restent fonctionnels.
- Erreur : Niveau 3, une erreur de périphérique s'est produite, par exemple un port étant hors ligne.
- **Avertissement** : Niveau 4, le niveau le plus bas d'un avertissement de périphérique.
- Avis : Niveau 5, fournit aux administrateurs réseau des informations sur le périphérique.
- **Information** : Niveau 6, fournit des informations sur le périphérique.
- Débogage Niveau 7, fournit des informations détaillées sur le journal.

7. Cliquez sur le bouton **Add** (Ajouter).

Le serveur syslog est ajouté.

Le champ Status du tableau Server Configuration indique si le serveur syslog est actuellement actif.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Modifiez les paramètres d'un serveur syslog

Pour modifier les paramètres d'un hôte syslog distant :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **surveillance > journaux > Journal du serveur** .

La page Journal du serveur s'affiche.

6. Cochez la case associée au serveur syslog.
7. Modifiez les paramètres en fonction de vos besoins.
8. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

Supprimez les paramètres d'un serveur syslog

Pour supprimer les paramètres d'un hôte syslog distant :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à

[Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **surveillance > journaux > Journal du serveur** .

La page Journal du serveur s'affiche.

6. Cochez la case associée au serveur syslog.

7. Cliquez sur le bouton **Supprimer**.

Le serveur syslog est supprimé.

Journal des interruptions :

Le journal des interruptions inclut des informations sur les interruptions envoyées par le commutateur. Vous pouvez afficher et effacer les entrées du journal des interruptions.

Vous pouvez également récupérer le journal des interruptions et enregistrer informatique sous forme de fichier. Pour plus d'informations, consultez [Exporter un fichier à partir du commutateur](#) . à la page 1145.

Pour afficher ou effacer le journal des interruptions :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **surveillance > journaux > journaux d'interruptions**.

La page journaux des interruptions s'affiche.

6. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).
7. Pour effacer les entrées du journal, cliquez sur le bouton **Clear Log** (Effacer le journal).
8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 192 : Informations du journal des interruptions

Champ	Description
Nombre d'interruptions depuis la dernière réinitialisation	Nombre d'interruptions qui se sont produites depuis le dernier redémarrage du commutateur.
Capacité du journal d'interruptions	Nombre maximal d'interruptions stockées dans le journal. Si le nombre d'interruptions dépasse la capacité, les nouvelles entrées remplacent les entrées les plus anciennes.
Nombre d'interruptions depuis la dernière consultation du journal	Nombre de recouvrements survenus depuis la dernière fois que les recouvrements ont été affichés.
 Remarque: Si vous enregistrez le journal des interruptions sur un autre périphérique (c'est-à-dire si vous téléchargez le fichier à partir du commutateur), ce compteur est défini sur 0.	

Table 192 : Informations du journal des interruptions (A continué)

Champ	Description
Journal	Numéro de séquence de cette trappe.
Durée de fonctionnement du système	Durée de cette interruption, exprimée en jours, heures, minutes et secondes, depuis le dernier redémarrage du commutateur.
Piège	Informations sur le piège.

Journaux des événements

Vous pouvez afficher et effacer le journal des événements, qui contient les messages d'erreur du commutateur.

❗ Remarque: Si vous rétablissez les paramètres par défaut du commutateur, le journal des événements n'est pas effacé.

Pour afficher ou effacer le journal des événements :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **surveillance > journaux > journaux d'événements**.

La page journaux des événements s'affiche.

6. Pour actualiser la page journal, cliquez sur le bouton **Refresh** (Actualiser).
7. Pour effacer les entrées du journal, cliquez sur le bouton **Clear Log** (Effacer le journal).
8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les informations du journal des événements affichées sur la page.

Table 193 : Informations sur les journaux d'événements

Champ	Description
Entrées	Numéro de séquence de l'événement.
Type	Type de l'événement.
Nom du fichier	Fichier d'origine de l'événement.
Ligne	Numéro de ligne de l'événement.
ID tâche	ID de tâche de l'événement.
Code	Le code incident.
Heure	Heure à laquelle cet événement s'est produit.

Configurer la journalisation USB

Si vous connectez un périphérique de stockage USB tel qu'un lecteur flash au commutateur, le commutateur enregistre les messages sur le périphérique.

Pour configurer la journalisation USB :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **surveillance > journaux > Configuration du journal USB**.

La page Configuration du journal USB s'affiche.

6. Dans le menu **USB Log mode**, sélectionnez le mode de consignation :

- **Écraser sur full** : Le commutateur enregistre les messages sur le périphérique USB et écrase les anciens messages si le périphérique USB est plein. Il s'agit de l'option par défaut.
- **Arrêt sur Full** : Le commutateur enregistre les messages sur le périphérique USB et arrête la journalisation si le périphérique USB est plein.
- Désactiver : Empêchez le commutateur d'enregistrer des messages sur le périphérique USB.

7. Dans le menu **USB Log mode**, sélectionnez le niveau de journalisation des messages à consigner.

Les messages de journal avec le niveau de gravité sélectionné et tous les messages de journal de gravité supérieure sont consignés. Par exemple, si vous sélectionnez **avertissement**, les messages consignés incluent avertissement, erreur, critique, alerte et urgence. Le niveau de gravité par défaut est Error (erreur) (3).

La gravité peut être l'un des niveaux suivants :

- Urgence Niveau 0, le niveau d'avertissement le plus élevé. Si le périphérique est en panne ou ne fonctionne pas correctement, un journal d'urgence est enregistré sur le périphérique.
- Avertir Niveau 1, le deuxième niveau d'avertissement le plus élevé. Un journal d'alertes est enregistré en cas de dysfonctionnement grave de l'appareil, par exemple en cas de panne de toutes les fonctions de l'appareil.
- **Critique**. Niveau 2, le troisième niveau d'avertissement le plus élevé. Un journal critique est enregistré en cas de dysfonctionnement critique d'un périphérique,

par exemple lorsque deux ports de périphérique ne fonctionnent pas, tandis que les autres ports de périphérique restent fonctionnels.

- Erreur : Niveau 3, une erreur de périphérique s'est produite, par exemple un port étant hors ligne.
- **Avertissement** : Niveau 4, le niveau le plus bas d'un avertissement de périphérique.
- Avis : Niveau 5, fournit aux administrateurs réseau des informations sur le périphérique. Il s'agit de l'option par défaut.
- **Information** : Niveau 6, fournit des informations sur le périphérique.
- Débogage Niveau 7, fournit des informations détaillées sur le journal.

❗ **Remarque:** Un journal enregistre les messages égaux ou supérieurs à un seuil de gravité configuré.

8. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

Le champ État opérationnel du journal USB affiche si la journalisation est activée (active ou inactive).

9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Port mirroring

La mise en miroir des ports vous permet de sélectionner le trafic réseau de ports de commutateur spécifiques pour analyse par un analyseur de réseau. Pour chaque configuration de mise en miroir de ports (le commutateur prend en charge jusqu'à quatre ports), vous pouvez sélectionner plusieurs ports de commutateur comme ports source, mais un seul port de commutateur comme port de destination. Pour chaque configuration de mise en miroir de port, vous pouvez configurer la manière dont le trafic est mis en miroir sur un port source en sélectionnant les paquets reçus, transmis ou les deux. Vous pouvez également appliquer une ACL IP ou MAC pour filtrer le trafic mis en miroir.

Un paquet copié sur le port de destination a le même format que le paquet d'origine. Cela signifie que si le miroir copie un paquet reçu, le paquet copié est étiqueté VLAN ou non car informatique a été reçu sur le port source. Si le miroir copie un paquet transmis, le paquet copié est étiqueté VLAN ou non car informatique est transmis sur le port source.

Pour définir une configuration de mise en miroir des ports :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **Monitoring > Mirroring > multiple Port Mirroring**.

La page mise en miroir de ports multiples s'affiche.

6. Dans le menu **ID de session**, sélectionnez **1**, **2**, **3** ou **4** comme ID de session de mise en miroir des ports.

Vous pouvez configurer quatre configurations de mise en miroir de ports qui fonctionnent indépendamment les unes des autres.

7. Activez ou désactivez la configuration de la mise en miroir des ports en sélectionnant l'un des boutons radio mode Admin suivants :

- **Vrai** Les interfaces source sélectionnées sont mises en miroir. Autrement dit, le trafic entrant ou sortant des interfaces sources est copié (mis en miroir) sur le port de destination sélectionné.
- **Faux** Les interfaces source sélectionnées ne sont pas mises en miroir.

8. Dans le menu **Port de destination**, sélectionnez l'interface de destination vers laquelle le trafic doit être copié.

Pour chaque configuration de mise en miroir de port, vous ne pouvez configurer qu'un seul port de destination. La valeur par défaut est aucun.

9. Dans le menu **type de filtre**, sélectionnez si le trafic doit être filtré :

- **Aucun** : Tout le trafic est mis en miroir.
- **IP ACL** : Le trafic est filtré en fonction de la liste de contrôle d'accès IP pour laquelle vous devez saisir le nom dans le champ **nom du filtre**. Seul le trafic qui correspond aux règles de la liste de contrôle d'accès IP est mis en miroir sur le port de destination.

Pour plus d'informations sur IP WiFi, voir Configurez une liste de contrôle d'accès IPv4 de base ou étendue, à la page 1049.

- **Liste de contrôle d'accès (ACL) MAC** Le trafic est filtré en fonction de la liste de contrôle d'accès MAC pour laquelle vous devez saisir le nom dans le champ **nom du filtre**. Seul le trafic qui correspond aux règles de la liste de contrôle d'accès MAC est mis en miroir sur le port de destination.

Pour plus d'informations sur les listes de contrôle d'accès MAC, reportez-vous à la section Configurez une ACL MAC, à la page 1036.

Les étapes suivantes font référence à la section Configuration de l'interface source, dans laquelle vous devez sélectionner une ou plusieurs interfaces source et définir la direction du trafic.

10. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :

- **1 ou ID d'unité pour un commutateur empilé** :
 - 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
 - **ID d'unité pour un commutateur empilé** : Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
- **LAG** Seuls les LAG sont affichés.
- **Processeur** Seule la CPU est affichée.
- **VLAN** Seuls les VLAN sont affichés.
- **Tous** : Les interfaces physiques, les LAG, le CPU et les VLAN sont affichés, ou pour une pile de commutateurs, les interfaces physiques de tous les commutateurs de la pile, les LAG, le CPU et les VLAN sont affichés.

11. Utilisez l'une des méthodes suivantes pour sélectionner une interface :

- Dans le champ **aller à l'interface**, entrez l'interface au format unité/emplacement/port et cliquez sur le bouton **aller**.
- En regard de la colonne interface, cochez la case correspondant à l'interface ou aux interfaces que vous souhaitez inclure.

❗ **Remarque:** Si une interface est membre d'un VLAN et d'un lag, vous ne pouvez pas sélectionner le VLAN comme VLAN source. Toutefois, si une interface est membre d'un VLAN que vous sélectionnez comme VLAN source, elle peut être membre d'un lag.

12. Dans le menu **Direction**, sélectionnez la direction du trafic qui doit être mis en miroir à partir des ports source configurés.

- **Aucun** : Le port (ou VLAN) n'est pas mis en miroir.
- **TX et Rx** : Le trafic de sortie (transmis) et de sortie (reçu) est mis en miroir. Pour un VLAN, cette option permet de sélectionner le VLAN comme VLAN source.
- **Réception** Seul le trafic d'entrée (reçu) est mis en miroir. Cette option n'est pas disponible pour un VLAN.
- **Transmission** Seul le trafic de sortie (transmis) est mis en miroir. Cette option n'est pas disponible pour un VLAN.

13. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

Si le port est configuré en tant que port source, le champ Status affiche Mirrored.

Si le port est configuré comme port de destination, le champ État affiche sonde.

14. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

VLAN RSPAN et commutateurs source et de destination

Vous pouvez configurer un VLAN en tant qu'analyseur de port commuté distant (RSPAN) VLAN. RSPAN vous permet de mettre en miroir le trafic provenant de plusieurs ports sources (ou de tous les ports membres d'un VLAN) provenant de différents périphériques réseau et d'envoyer le trafic mis en miroir à un port de destination (port de sonde connecté à un analyseur de réseau) sur un périphérique distant. Le trafic mis en miroir est étiqueté avec l'ID VLAN RSPAN et transmis sur les ports de jonction dans le VLAN RSPAN.

Un commutateur peut fonctionner comme un commutateur source RSPAN qui envoie le trafic à un autre commutateur qui fonctionne comme un commutateur de destination RSPAN. Comme le commutateur prend en charge plusieurs configurations RSPAN, il peut également fonctionner comme un commutateur de destination RSPAN qui reçoit le trafic d'un autre commutateur qui fonctionne comme un commutateur source RSPAN.

Configurer un VLAN existant en tant que VLAN RSPAN

Vous pouvez configurer un VLAN existant en tant que VLAN RSPAN.

Pour configurer un VLAN existant en tant que VLAN RSPAN :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **surveillance > mise en miroir > VLAN RSPAN**.

La page VLAN RSPAN s'affiche.

6. Cochez la case du VLAN qui doit devenir un VLAN RSPAN.

7. Dans le menu **mode Admin**, sélectionnez **Activer** pour configurer le VLAN en tant que VLAN RSPAN.
Par défaut, la sélection est désactiver et le VLAN n'est pas un VLAN RSPAN.
8. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
9. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez le commutateur en tant que commutateur source RSPAN

Vous pouvez configurer le commutateur en tant que commutateur source RSPAN qui envoie le trafic à un autre commutateur qui fonctionne comme commutateur de destination RSPAN.

Vous pouvez créer jusqu'à quatre configurations de commutateur source RSPAN.

Pour configurer le commutateur en tant que commutateur source RSPAN :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
 - Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
 - Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur principale à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **surveillance > mise en miroir > Configuration du commutateur source RSPAN**.

La page Configuration du commutateur source RSPAN s'affiche.

6. Dans le menu **ID de session**, sélectionnez **1**, **2**, **3** ou **4** comme ID de session du commutateur source RSPAN.

Vous pouvez configurer quatre configurations de commutateur source RSPAN qui fonctionnent indépendamment les unes des autres.

7. Activez ou désactivez la configuration du commutateur source RSPAN en sélectionnant l'un des boutons radio Admin mode suivants :

- **Vrai** Les interfaces source sélectionnées sont mises en miroir. Autrement dit, le trafic entrant ou sortant des interfaces sources est copié (mis en miroir) sur le VLAN de destination RSPAN sélectionné.
- **Faux** Les interfaces source sélectionnées ne sont pas mises en miroir.

8. Dans le menu **VLAN de destination RSPAN**, sélectionnez le VLAN de destination vers lequel le trafic doit être copié.

Pour chaque configuration de commutateur source RSPAN, vous pouvez configurer un seul port VLAN de destination RSPAN. La valeur par défaut est aucun.

9. Dans le menu **RSPAN Reflector Port**, sélectionnez l'interface connectée au commutateur de destination RSPAN.

10. Dans le menu **type de filtre**, sélectionnez si le trafic doit être filtré :

- **Aucun** : Tout le trafic est envoyé au VLAN de destination.
- **IP ACL** : Le trafic est filtré en fonction de la liste de contrôle d'accès IP pour laquelle vous devez saisir le nom dans le champ **nom du filtre**. Seul le trafic qui correspond aux règles de la liste de contrôle d'accès IP est envoyé au VLAN de destination.

Pour plus d'informations sur IP WiFi, voir Configurez une liste de contrôle d'accès IPv4 de base ou étendue, à la page 1049.

- **Liste de contrôle d'accès (ACL) MAC** Le trafic est filtré en fonction de la liste de contrôle d'accès MAC pour laquelle vous devez saisir le nom dans le champ **nom du filtre**. Seul le trafic qui correspond aux règles de la liste de contrôle d'accès MAC est envoyé au VLAN de destination.

Pour plus d'informations sur les listes de contrôle d'accès MAC, reportez-vous à la section Configurez une ACL MAC, à la page 1036.

Les étapes suivantes font référence à la section Configuration de l'interface source RSPAN, dans laquelle vous devez sélectionner une ou plusieurs interfaces source et définir la direction du trafic.

11. Choisissez d'afficher les interfaces physiques, les LAG ou les deux en cliquant sur l'un des liens suivants au-dessus de l'en-tête du tableau :

- **1 ou ID d'unité pour un commutateur empilé :**
 - 1. Si aucune pile de commutateurs n'est configurée, les interfaces physiques du commutateur sont affichées.
 - **ID d'unité pour un commutateur empilé :** Si une pile de commutateurs est configurée, les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
- LAG Seuls les LAG sont affichés.
- Processeur Seule la CPU est affichée.
- VLAN Seuls les VLAN sont affichés.
- **Tous:** Les interfaces physiques, les LAG, le CPU et les VLAN sont affichés, ou pour une pile de commutateurs, les interfaces physiques de tous les commutateurs de la pile, les LAG, le CPU et les VLAN sont affichés.

12. Utilisez l'une des méthodes suivantes pour sélectionner une interface :

- Dans le champ **aller à l'interface**, entrez l'interface au format unité/emplacement/port et cliquez sur le bouton **aller**.
- En regard de la colonne interface, cochez la case correspondant à l'interface ou aux interfaces que vous souhaitez inclure.

❗ Remarque: Si une interface est membre d'un VLAN et d'un lag, vous ne pouvez pas sélectionner le VLAN comme VLAN source. Toutefois, si une interface est membre d'un VLAN que vous sélectionnez comme VLAN source, elle peut être membre d'un lag.

13. Dans le menu **Direction**, sélectionnez la direction du trafic qui doit être mis en miroir à partir des ports source configurés.

- **Aucun :** Le port (ou VLAN) n'est pas mis en miroir.
- **TX et Rx :** Le trafic de sortie (transmis) et de sortie (reçu) est mis en miroir. Pour un VLAN, cette option permet de sélectionner le VLAN comme VLAN source.
- **Réception** Seul le trafic d'entrée (reçu) est mis en miroir. Cette option n'est pas disponible pour un VLAN.
- **Transmission** Seul le trafic de sortie (transmis) est mis en miroir. Cette option n'est pas disponible pour un VLAN.

14. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

Si le port est configuré en tant que port source, le champ Status affiche Mirrored.

15. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurez le commutateur en tant que commutateur de destination RSPAN

Vous pouvez configurer le commutateur en tant que commutateur de destination RSPAN qui reçoit le trafic d'un autre commutateur fonctionnant comme commutateur source RSPAN.

Vous pouvez créer jusqu'à quatre configurations de commutateur de destination RSPAN.

Pour configurer le commutateur en tant que commutateur de destination RSPAN :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **surveillance > mise en miroir > Configuration du commutateur de destination RSPAN**.

La page Configuration du commutateur de destination RSPAN s'affiche.

6. Dans le menu **ID de session**, sélectionnez **1**, **2**, **3** ou **4** comme ID de session du commutateur de destination RSPAN.

Vous pouvez configurer quatre configurations de commutateur de destination RSPAN qui fonctionnent indépendamment les unes des autres.

7. Activez ou désactivez la configuration du commutateur de destination RSPAN en sélectionnant l'un des boutons radio Admin mode suivants :

- **Vrai** Le trafic provenant du VLAN source RSPAN sélectionné est copié (mis en miroir) sur le port de destination RSPAN sélectionné.
- **Faux** Le trafic provenant du VLAN source RSPAN sélectionné n'est pas mis en miroir.

8. Dans le menu **RSPAN source VLAN**, sélectionnez l'VLAN source RSPAN à partir duquel le trafic doit être copié.

9. Dans le menu **Port de destination RSPAN**, sélectionnez le port de destination RSPAN vers lequel le trafic doit être copié.

Pour chaque configuration de commutateur de destination RSPAN, vous pouvez configurer un seul port de destination RSPAN. La valeur par défaut est aucun.

10. Dans le menu **type de filtre**, sélectionnez si le trafic doit être filtré :

- **Aucun** : Tout le trafic est envoyé au port de destination RSPAN.
- **IP ACL** : Le trafic est filtré en fonction de la liste de contrôle d'accès IP pour laquelle vous devez saisir le nom dans le champ **nom du filtre**. Seul le trafic qui correspond aux règles de la liste de contrôle d'accès IP est envoyé au port de destination RSPAN.

Pour plus d'informations sur IP WiFi, voir [Configurez une liste de contrôle d'accès IPv4 de base ou étendue](#), à la page 1049.

- **Liste de contrôle d'accès (ACL) MAC** Le trafic est filtré en fonction de la liste de contrôle d'accès MAC pour laquelle vous devez saisir le nom dans le champ **nom du filtre**. Seul le trafic qui correspond aux règles de la liste de contrôle d'accès MAC est envoyé au port de destination RSPAN.

Pour plus d'informations sur les listes de contrôle d'accès MAC, reportez-vous à la section [Configurez une ACL MAC](#), à la page 1036.

11. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

12. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Surveillance SFlow

SFlow est une norme de surveillance des réseaux commutés et routés à haut débit. La technologie sFlow est intégrée au commutateur et à de nombreux autres périphériques réseau pour offrir une visibilité sur l'activité du réseau.

Le système de surveillance sFlow se compose d'un agent sFlow intégré et d'un collecteur sFlow central, également appelé récepteur sFlow. L'agent sFlow utilise la technologie d'échantillonnage pour capturer les statistiques de trafic du périphérique surveillé par informatique. Les datagrammes sFlow sont utilisés pour transmettre les statistiques de trafic échantillonnées à un collecteur sFlow pour analyse.

L'agent sFlow utilise deux formes d'échantillonnage : l'échantillonnage statistique par paquets des flux de paquets commutés ou routés, et l'échantillonnage temporel des compteurs.

Présentation de l'agent sFlow

L'échantillonnage de flux de paquets et le contre-échantillonnage sont effectués par des instances sFlow associées à des sources de données individuelles au sein de l'agent sFlow. Les échantillons de flux de paquets et les échantillons de compteur sont combinés dans des datagrammes sFlow. L'échantillonnage de flux de paquets provoque l'envoi d'un flux régulier mais aléatoire de datagrammes sFlow au collecteur sFlow. Des échantillons de compteur peuvent être prélevés de manière opportuniste pour remplir ces datagrammes.

Pour effectuer un échantillonnage de flux de paquets, vous devez configurer une instance d'échantillonneur sFlow avec une fréquence d'échantillonnage. Pour effectuer un contre-échantillonnage, vous devez configurer une instance de poller sFlow avec un intervalle d'interrogation. L'agent sFlow envoie les informations collectées sous forme de datagrammes sFlow aux collecteurs sFlow au récepteur sFlow.

Configurez l'interface source pour l'agent sFlow

Le commutateur peut fonctionner comme un agent sFlow et transmettre le trafic interrogé et échantillonné à un récepteur sFlow. Vous pouvez configurer l'interface source qui se connecte au périphérique qui fonctionne comme récepteur sFlow.

Pour configurer l'interface source de l'agent sFlow :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **surveillance> sFlow > basique > informations sur l'agent sFlow** .

La page informations sur l'agent sFlow s'affiche.

6. Dans le menu **interface source**, sélectionnez l'interface de gestion que l'agent sFlow doit utiliser. Par défaut, les options suivantes s'affichent dans le menu :

- **Aucun** : L'adresse IP principale de l'interface d'origine (sortante) est utilisée comme adresse source.
- **VLAN 1** L'adresse IP principale de VLAN 1 est utilisée comme adresse source. Il s'agit de la sélection par défaut.
- **Port de service** L'adresse IP du port de gestion est utilisée comme adresse source.

Selon la configuration de votre commutateur, les options suivantes peuvent s'afficher :

- **Un autre identifiant VLAN** : L'adresse IP principale d'un VLAN autre que VLAN 1 est utilisée comme adresse source.
- **Interface de routage** : L'adresse IP principale d'une interface de routage est utilisée comme adresse source.
- **VLAN de routage** L'adresse IP principale d'une interface de routage VLAN est utilisée comme adresse source.

- **Interface de bouclage de routage** : L'adresse IP principale d'une interface de bouclage de routage est utilisée comme adresse source.
- **Différent**: Pour certaines fonctionnalités, *différents* peuvent s'afficher. Cela signifie que l'interface source est configurée séparément.

7. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 194 : Informations sur l'agent sFlow

Champ	Description
"Version de l'agent"	La version et la mise en œuvre de la MIB. La version de l'agent comprend les composants suivants : • Version MIB : Par exemple, 1,3. • Entreprise : NETGEAR • Révision : Par exemple, 13.0,2.10.
Adresse de l'agent	Adresse IP associée à l'agent. L'adresse IP dépend de votre sélection de l'interface source.

Configurer un récepteur sFlow

Vous pouvez configurer un ou plusieurs périphériques qui doivent fonctionner comme récepteurs sFlow. L'interface source sFlow assure la connexion à ces périphériques.

Pour configurer un récepteur sFlow :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **surveillance > sFlow > Avancé > Configuration du récepteur sFlow**.

La page Configuration du récepteur sFlow s'affiche.

6. Cochez la case **Index du récepteur** pour un récepteur.
7. Dans le champ **propriétaire du récepteur**, spécifiez le propriétaire du récepteur. Spécifiez le nom du propriétaire ou du périphérique.

Par défaut, l'option de délai d'attente est activée, mais la période de délai d'attente est configurée sur 0, ce qui signifie que l'échantillonnage sFlow ne s'arrête pas après l'activation de informatique.

8. Pour configurer une période de temporisation, procédez comme suit :

- a. Dans le champ **délai du récepteur**, spécifiez le délai d'expiration en secondes après lequel l'échantillonnage s'arrête.

La plage est de 0 à 2147483647. Une valeur de zéro signifie que l'échantillonnage sFlow ne s'arrête pas après l'activation de informatique.

- b. Dans le menu **No Timeout**, sélectionnez **False** pour activer l'option Time-out Sampling.

La valeur par défaut est False. Si vous sélectionnez **vrai**, l'échantillonnage n'expire pas et la période de temporisation est automatiquement définie sur le maximum de 2147483647.

9. Dans le champ **taille maximale du datagramme**, spécifiez le nombre maximal d'octets de données pouvant être envoyés dans un seul exemple de datagramme. La valeur par défaut est 1400. La plage est de 200 à 12188. Pour éviter la fragmentation des datagrammes, nous vous recommandons de ne pas définir une taille de datagramme trop basse.

10. Dans le champ **adresse du récepteur**, spécifiez l'adresse IP du récepteur sFlow.

11. Dans le champ **Port du récepteur**, spécifiez le port de destination pour les datagrammes sFlow.
Le numéro de port par défaut est 6343. La plage est de 1 à 65535.
12. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
Le champ Receiver Datagram version affiche 5 comme version des datagrammes sFlow.
13. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurer l'interrogation et l'échantillonnage sFlow sur une interface

Si le commutateur est configuré en tant qu'agent sFlow, il peut effectuer les opérations suivantes :

- Collecter des échantillons statistiques basés sur des paquets de flux commutés et les envoyer aux récepteurs configurés. Une source de données configurée pour collecter des échantillons de flux est appelée échantillonneur.
- Collectez l'échantillonnage temporel des statistiques d'interface réseau et envoyez-les aux récepteurs sFlow configurés. Une source de données configurée pour collecter des échantillons de compteur est appelée poller.

Vous pouvez configurer les paramètres d'échantillonnage et d'interrogation sur une interface de commutateur. Le trafic sur l'interface est ensuite échantillonné, interrogé et transmis au récepteur sFlow.

Pour configurer l'interrogation et l'échantillonnage sFlow sur une interface :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **surveillance > sFlow > Avancé > Configuration de l'interface sFlow**.

La page Configuration de l'interface sFlow s'affiche.

6. Si une pile est configurée, indiquez si vous souhaitez afficher les interfaces physiques d'un commutateur ou de tous les commutateurs de la pile :

- **ID d'unité pour un commutateur empilé** : Les interfaces physiques du commutateur avec l'ID d'unité de pile sélectionnée sont affichées.
Si aucune pile de commutateurs n'est configurée, la seule option est l'ID d'unité 1.
- **Tous** : Les interfaces physiques de tous les commutateurs de la pile sont affichées.
Si aucune pile de commutateurs n'est configurée, l'option tous n'a aucun effet.

7. Utilisez l'une des méthodes suivantes pour sélectionner une interface pour l'interrogateur de flux et l'échantillonneur :

- Dans le champ **aller à l'interface**, entrez l'interface au format unité/emplacement/port et cliquez sur le bouton **aller**.
- En regard de la colonne interface, cochez la case correspondant à l'interface que vous souhaitez utiliser.

Vous ne pouvez sélectionner que des ports physiques.

8. Dans le champ **Index du récepteur Poller**, spécifiez le récepteur sFlow qui doit être associé au sondeur.

Pour plus d'informations sur les récepteurs sFlow, voir [Configurer un récepteur sFlow](#) à la page 1132.

9. Dans le champ **intervalle d'interrogation**, spécifiez le nombre de secondes entre les interrogations successives.

Un intervalle d'échantillonnage de 0 désactive l'échantillonnage. La plage est de 0 à 86400 secondes. La valeur par défaut est 0 seconde.

10. Dans le champ **Index du récepteur de l'échantillonneur**, spécifiez le récepteur sFlow qui doit être associé à l'échantillonneur.

Pour plus d'informations sur les récepteurs sFlow, voir [Configurer un récepteur sFlow](#) à la page 1132.

11. Dans le champ **Sampling Rate**, spécifiez le taux d'échantillonnage statistique pour l'échantillonnage des paquets.

Un taux d'échantillonnage de 1 compte tous les paquets. Un taux d'échantillonnage de 0 désactive l'échantillonnage. La plage autorisée est de 1024 à 65536. Le numéro par défaut est 0.

12. Dans le champ **taille maximale de l'en-tête**, spécifiez le nombre maximal d'octets à copier à partir d'un paquet échantillonné.

La plage est de 20 à 256 secondes. La valeur par défaut est 128 octets.

13. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

14. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

11

Maintenance et dépannage

Ce chapitre aborde les sujets suivants :

- Enregistrez la configuration
- Installation automatique du fichier de configuration
- Redémarrez le commutateur à partir de l'interface utilisateur principale
- Pour rétablir les paramètres par défaut du routeur :
- Exporter un fichier à partir du commutateur .
- Mettez à jour le logiciel ou téléchargez un fichier
- Gérer les images logicielles .
- Diagnostics et dépannage

Enregistrez la configuration

Lorsque vous enregistrez la configuration, les modifications que vous avez apportées sont conservées par le commutateur au redémarrage de l'informatique. Vous pouvez également enregistrer les paramètres sur chaque page de configuration de l'interface utilisateur principale en cliquant sur l'icône **Enregistrer**.

Pour enregistrer la configuration :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **maintenance > Enregistrer la configuration > Enregistrer la configuration**.

La page Enregistrer la configuration s'affiche.

6. Cochez la case.

7. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés. Si vous redémarrez le commutateur, les paramètres enregistrés sont conservés.

Installation automatique du fichier de configuration

Si le commutateur est initialisé sans fichier de configuration, le processus d'installation automatique (installation automatique) peut charger automatiquement la configuration du commutateur à partir d'un serveur du réseau.

Configurez le processus d'installation automatique

Le processus d'installation automatique nécessite que DHCP soit activé par défaut sur le commutateur. Pour enregistrer la configuration téléchargée dans la configuration de démarrage, vous devez enregistrer explicitement le fichier en tant que tel. Le processus d'installation automatique dépend de la configuration des autres périphériques du réseau, y compris un serveur DHCP ou BOOTP, un serveur TFTP et, si nécessaire, un serveur DNS.

Le processus d'installation automatique se déroule en trois phases :

1. **Configuration ou attribution d'une adresse IP au commutateur** : Pour plus d'informations, voir [Interfaces de gestion IPv4 et VLAN](#) à la page 99 ou [Interfaces de gestion IPv6 et VLAN](#) à la page 106.
2. **Affectation d'un serveur TFTP** : Si le commutateur fonctionne comme un client DHCP (ce que l'ordinateur fait par défaut), le serveur DHCP peut automatiquement fournir le serveur TFTP au commutateur, par exemple, si le serveur DHCP est configuré avec l'option 125 (voir [Option 125 serveur DHCP requis pour obtenir un fichier de configuration via l'installation automatique](#) à la page 1141).
3. **Téléchargement d'un fichier de configuration pour le commutateur à partir du serveur TFTP** : Reportez-vous à la procédure suivante.

Pour configurer le processus d'installation automatique :

- a. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
La page de connexion s'affiche.
- b. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
- c. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

d. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

e. Sélectionnez **maintenance > Enregistrer la configuration > Configuration de l'installation automatique**.

La page Configuration de l'installation automatique s'affiche.

f. Dans le menu **mode installation automatique**, sélectionnez pour démarrer ou arrêter le processus d'installation automatique :

- **Démarrer**. Démarre le processus d'installation automatique (après avoir cliqué sur le bouton **appliquer**).
- **Stop** (Arrêter) - Arrête le processus d'installation automatique (après avoir cliqué sur le bouton **appliquer**).

g. Dans le menu **AutoInstall persistent mode**, sélectionnez pour activer ou désactiver le mode persistant pour le processus d'installation automatique :

- Sous tension Le processus d'installation automatique enregistre le fichier de configuration téléchargé et applique informatique après le redémarrage du commutateur. Il s'agit de l'option par défaut.
- Désactivé : Le processus d'installation automatique n'enregistre pas le fichier de configuration téléchargé et, par conséquent, ne peut pas appliquer informatique après le redémarrage du commutateur.

h. Dans le menu **mode d'enregistrement automatique**, sélectionnez pour activer ou désactiver l'enregistrement automatique de la configuration dans la configuration de démarrage :

- Sous tension La configuration téléchargée automatiquement est enregistrée dans la configuration de démarrage.
- Désactivé : La configuration téléchargée automatiquement n'est pas enregistrée dans la configuration de démarrage. Si vous souhaitez enregistrer la configuration, vous devez effectuer manuellement. Il s'agit de l'option par défaut.

- i. Dans le menu **nombre de tentatives d'installation automatique**, spécifiez le nombre de fois que le commutateur envoie un message de monodiffusion au serveur TFTP.

Le serveur TFTP est spécifié dans la configuration DHCP (voir [Option 125 serveur DHCP requis pour obtenir un fichier de configuration via l'installation automatique](#) à la page 1141). Une fois le nombre de fois spécifié dépassé, le commutateur envoie des messages de diffusion au serveur TFTP. La plage est de 1 à 3. Par défaut, le nombre est 3.

- j. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

Le champ État de l'installation automatique affiche l'état du processus d'installation automatique.

Option 125 serveur DHCP requis pour obtenir un fichier de configuration via l'installation automatique

Vous pouvez utiliser l'installation automatique pour permettre au commutateur de télécharger un fichier de configuration (fichier image) à partir d'un serveur TFTP à l'aide de l'option DHCP 125. La mise à jour de l'image peut mettre à niveau ou rétrograder le micrologiciel sur le commutateur.

Pour que le commutateur puisse télécharger une image à partir d'un serveur TFTP, le serveur DHCP doit inclure un fichier de description d'image qui répertorie l'image que le commutateur doit télécharger à partir du serveur TFTP. Par exemple, le fichier de description d'image `autoinstall_dhcp` sur le serveur DHCP répertorie l'image `M4XXX-v1.2.3.4.stk` que le commutateur doit télécharger à partir du serveur TFTP.

L'option 125 du serveur DHCP doit contenir les informations suivantes (l'exemple utilise le fichier de description d'image `autoinstall_dhcp` et l'image `M4XXX-v1.2.3.4.stk`) :

- **Numéro d'entreprise (4 octets)**. 0x0000 0x11ae

En décimales, le numéro d'entreprise de NETGEAR est 4526.

- **Longueur des données (1 octet)** : 0x12

La longueur des données inclut le code de la sous-option, la longueur de la sous-option et le fichier de description de l'image (et non l'image elle-même) :
1+1+16

- **Code de sous-option (2 octets) :** 0x05
- **Longueur de la sous-option (1 octet) :** 0x10
Longueur du nom du fichier de description d'image.
- **Nom du fichier de description de l'image (N octets) :**
61.7574.6f69.6e73.7461.6c6c.5f64.6863.70
En texte brut, le nom du fichier de description d'image est `autoinstall_dhcp`.

Le contenu du fichier de description d'image `autoinstall_dhcp` est `M4XXX-v1.2.3.4.stk`, qui est l'image que le commutateur doit télécharger à partir du serveur TFTP.

Vous pouvez modifier le nom du fichier de description d'image, mais vous devez également modifier la longueur de données de l'option 125, qui est basée sur le code de la sous-option, la longueur de la sous-option et le nom du fichier de description d'image.

Redémarrez le commutateur à partir de l'interface utilisateur principale

Vous pouvez redémarrer le commutateur à partir de l'interface utilisateur principale. Si votre configuration inclut une pile de commutateurs, vous pouvez sélectionner le commutateur à redémarrer ou redémarrer tous les commutateurs de la pile.

❗ Remarque : Si vous pouvez physiquement accéder au commutateur, vous pouvez le redémarrer en appuyant sur le bouton de **réinitialisation** multifonction situé sur le panneau avant pendant moins de 5 secondes. (N'appuyez pas sur le bouton pendant plus de 5 secondes !)

Pour redémarrer le commutateur :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **maintenance > Réinitialiser > redémarrage du périphérique**.

La page Device Reboot s'affiche.

6. Dans le menu Reboot Unit N°, sélectionnez le commutateur à redémarrer ou sélectionnez **All** pour redémarrer tous les commutateurs d'une pile.

Si votre commutateur ne fonctionne pas dans une pile, sélectionnez **1**.

7. Sélectionnez l'une des cases d'option suivantes :

- **Enregistrer avant le redémarrage** : Le commutateur enregistre toutes les modifications que vous avez effectuées et pour lesquelles vous n'avez pas cliqué sur l'icône **Enregistrer** dans l'interface principale.
- **Ne pas enregistrer avant le redémarrage** : Le commutateur n'enregistre pas les modifications que vous avez effectuées et pour lesquelles vous n'avez pas cliqué sur l'icône **Enregistrer** dans l'interface principale.

8. Cliquez sur le bouton **Apply** (Appliquer).

Une fenêtre contextuelle alerte s'affiche.

9. d. cliquez sur le bouton OK pour confirmer.

Le commutateur redémarre.

Pour rétablir les paramètres par défaut du routeur :

Vous pouvez rétablir les valeurs par défaut de la configuration du commutateur. Toutes les modifications que vous avez apportées sont effacées. Si l'adresse IP change, votre session Web risque de se déconnecter.

❗ Remarque: Si vous réinitialisez la configuration par défaut du commutateur, l'adresse IP de gestion est réinitialisée sur 169.254.100.100, et le client DHCP est activé. Aucune adresse IP n'est définie pour le port OOB, mais son client DHCP est activé. Si vous perdez la connectivité réseau après avoir réinitialisé les paramètres par défaut du commutateur, reportez-vous à la section [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33.

Pour rétablir les paramètres par défaut du routeur :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **maintenance > Réinitialiser > Paramètres usine par défaut**.

La page PAR DÉFAUT s'affiche.

6. Cochez la case.

7. Cliquez sur le bouton **Apply** (Appliquer).

Une fenêtre contextuelle de confirmation s'affiche.

8. d. cliquez sur le bouton OK pour confirmer.

La configuration est réinitialisée aux paramètres par défaut.

Exporter un fichier à partir du commutateur .

Vous pouvez exporter des fichiers de configuration (ASCII) ou journaux (ASCII log) du commutateur vers un serveur de fichiers via une session TFTP, SFTP, SCP ou FTP, vers un ordinateur via une session HTTP ou vers un périphérique de stockage USB.

Exporter un fichier du commutateur vers un serveur

Vous pouvez télécharger (exporter) la configuration (ASCII ou log ASCII) et d'autres types de fichiers du commutateur vers un serveur TFTP, SFTP, SCP ou FTP du réseau.

Pour exporter un fichier du commutateur vers un serveur :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **maintenance > Exporter > exportation de fichiers HTTP**.

La page exportation de fichiers HTTP s'affiche.

6. Dans le menu **type de fichier**, sélectionnez le type de fichier à exporter :

- **Configuration du texte** : Un fichier de configuration basé sur du texte vous permet de modifier un fichier texte configuré (`startup-config`) hors ligne selon vos besoins. L'utilisation la plus courante de la configuration textuelle est de télécharger une configuration de travail à partir d'un périphérique, de la modifier hors ligne pour la personnaliser pour un autre périphérique similaire (par exemple, changer le nom du périphérique ou l'adresse IP), et de la télécharger sur ce périphérique. Il s'agit de l'option par défaut.
- **Journal d'erreurs** : Journal persistant des erreurs du commutateur, également appelé journal des événements.
- **Journal tamponné** : Journal mis en mémoire tampon du système.
- **Journal des interruptions** : Le journal des interruptions avec les enregistrements des interruptions de commutation.
- **Fichier script** : Le fichier script que vous devez spécifier dans le champ **nom du fichier local**.
- **Bannière CLI** : Le fichier de bannière CLI.
- **Support technique**. Le fichier de support technique est un fichier texte qui contient une variété d'informations sur le matériel, les logiciels et la configuration qui peuvent aider au dépannage des périphériques et du réseau.
- **Journaux d'incidents** : Les journaux de plantage du commutateur, le cas échéant, sont disponibles.
- **CONFIGURATION DE LA SAUVEGARDE** Le fichier de configuration de sauvegarde est un fichier texte.

- **Fichier de capture des paquets CPU** : Les paquets CPU capturent le fichier avec les paquets CPU capturés et stockés.
 - **Configuration usine par défaut** : Le fichier de configuration usine par défaut est un fichier texte contenant la configuration usine par défaut enregistrée.
 - **Fichier de configuration du client DHCP** : Le fichier de configuration du client DHCP avec les informations du serveur DHCP (hôte).
7. Dans le menu **Transfer mode**, spécifiez le protocole à utiliser pour transférer le fichier vers le serveur :
- TFTP Protocole Trivial File Transfer.
 - SFTP Protocole de transfert de fichiers sécurisé. Cette sélection nécessite la spécification d'un nom d'utilisateur et d'un mot de passe.
 - **SCP**: Protocole de copie sécurisé. Cette sélection nécessite la spécification d'un nom d'utilisateur et d'un mot de passe.
 - **FTP**. Protocole de transfert de fichiers. Cette sélection nécessite la spécification d'un nom d'utilisateur et d'un mot de passe.
8. Dans le menu **type d'adresse du serveur**, sélectionnez le format du champ **adresse du serveur** :
- IPv4 : Indique que l'adresse du serveur est une adresse IPv4 au format décimal à points. Il s'agit de l'option par défaut.
 - IPv6 : Indique que l'adresse du serveur est une adresse IPv6 en nombres hexadécimaux utilisant des valeurs de 16 bits entre deux-points.
 - DNS : Indique que l'adresse du serveur est un nom d'hôte.
9. Dans le champ **adresse du serveur**, entrez l'adresse IP du serveur conformément au format indiqué par le type d'adresse du serveur.
L'adresse par défaut est l'adresse IPv4 0,0.0,0.
10. Dans le champ **chemin du fichier distant**, spécifiez le chemin sur le serveur où vous souhaitez enregistrer le fichier.
Le nom du chemin peut inclure uniquement des caractères alphabétiques, numériques, barre oblique, point ou trait de soulignement. Vous pouvez entrer jusqu'à 160 caractères.
11. Dans le champ **nom du fichier distant**, spécifiez un nom de fichier de destination pour le fichier à exporter.
Vous pouvez entrer jusqu'à 32 caractères.
12. Si vous sélectionnez **fichier script** dans le menu **type de fichier**, spécifiez le nom du fichier script dans la zone **nom du fichier local**.

13. Si vous sélectionnez **SFTP**, **SCP** ou **FTP** dans le menu **Transfer mode**, spécifiez les paramètres suivants :

- Nom d'utilisateur : Spécifiez le nom d'utilisateur pour la connexion à distance au serveur.
- Nouveau mot de passe : Spécifiez le mot de passe pour la connexion à distance au serveur.

14. Cliquez sur le bouton **Apply** (Appliquer).

Le fichier est exporté (téléchargé) vers l'ordinateur. La page affiche des informations sur la progression du transfert de fichier.

Utilisez HTTP pour exporter un fichier du commutateur vers un ordinateur

Vous pouvez télécharger (exporter) des fichiers de différents types depuis le commutateur vers un ordinateur via une session HTTP sur votre navigateur Web.

Pour utiliser HTTP pour exporter un fichier du commutateur vers un ordinateur :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **maintenance > Exporter > exportation de fichiers HTTP**.

La page exportation de fichiers HTTP s'affiche.

6. Dans le menu **type de fichier**, sélectionnez le type de fichier à exporter :

- **Configuration du texte** : Un fichier de configuration basé sur du texte vous permet de modifier un fichier texte configuré (**startup-config**) hors ligne selon vos besoins. L'utilisation la plus courante de la configuration textuelle est de télécharger une configuration de travail à partir d'un périphérique, de la modifier hors ligne pour la personnaliser pour un autre périphérique similaire (par exemple, changer le nom du périphérique ou l'adresse IP), et de la télécharger sur ce périphérique. Il s'agit de l'option par défaut.
- **Journal d'erreurs** : Journal persistant des erreurs du commutateur, également appelé journal des événements.
- **Journal tamponné** : Journal mis en mémoire tampon du système.
- **Journal des interruptions** : Le journal des interruptions avec les enregistrements des interruptions de commutation.
- **Fichier script** : Le fichier script que vous devez spécifier dans le champ **nom du fichier local**.
- **Bannière CLI** : Le fichier de bannière CLI.
- **Support technique**. Le fichier de support technique est un fichier texte qui contient une variété d'informations sur le matériel, les logiciels et la configuration qui peuvent aider au dépannage des périphériques et du réseau.
- **Journaux d'incidents** : Les journaux de plantage du commutateur, le cas échéant, sont disponibles.
- **CONFIGURATION DE LA SAUVEGARDE** Le fichier de configuration de sauvegarde est un fichier texte.
- **Fichier de capture des paquets CPU** : Les paquets CPU capturent le fichier avec les paquets CPU capturés et stockés.
- **Configuration usine par défaut** : Le fichier de configuration usine par défaut est un fichier texte contenant la configuration usine par défaut enregistrée.
- **Fichier de configuration du client DHCP** : Le fichier de configuration du client DHCP avec les informations du serveur DHCP (hôte).

7. Si vous sélectionnez **fichier script** dans le menu **type de fichier**, spécifiez le nom du fichier script dans la zone **nom du fichier local**.

8. Cliquez sur le bouton **Apply** (Appliquer).

Le fichier est exporté (téléchargé) vers l'ordinateur. La page affiche des informations sur la progression du transfert de fichier.

Exportez un fichier du commutateur vers un périphérique de stockage USB

Vous pouvez télécharger (exporter) un fichier de configuration texte ou un fichier de configuration client DHCP vers un périphérique de stockage USB connecté au commutateur.

Pour exporter un fichier du commutateur vers un périphérique de stockage USB :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **maintenance > Exporter > exportation de fichiers USB**.

La page exportation de fichiers USB s'affiche.

6. Dans le menu **type de fichier**, sélectionnez le type de fichier à exporter :

- **Configuration du texte** : Un fichier de configuration basé sur du texte vous permet de modifier un fichier texte configuré (**startup-config**) hors ligne selon vos besoins. L'utilisation la plus courante de la configuration textuelle est de télécharger une configuration de travail à partir d'un périphérique, de la modifier hors ligne pour la personnaliser pour un autre périphérique similaire (par exemple, changer le nom du périphérique ou l'adresse IP), et de la télécharger sur ce périphérique. Il s'agit de l'option par défaut.
 - **Fichier de configuration du client DHCP** : Le fichier de configuration du client DHCP avec les informations du serveur DHCP (hôte).
7. Dans le champ **chemin du fichier**, spécifiez le chemin sur le périphérique de stockage USB.
Vous pouvez entrer jusqu'à 146 caractères. La valeur par défaut est vide.
 8. Dans le champ **fichier USB**, spécifiez un nom pour le fichier. Il s'agit du nom sous lequel le fichier sera enregistré sur le périphérique de stockage USB.
Vous pouvez entrer jusqu'à 32 caractères.
 9. Cliquez sur le bouton **Apply** (Appliquer).
Le fichier est exporté (téléchargé) vers le périphérique de stockage USB. La page affiche des informations sur la progression du transfert de fichier.

Mettez à jour le logiciel ou téléchargez un fichier

Vous pouvez télécharger le micrologiciel, la configuration (ASCII), le journal (ASCII log), SSL, PEM ou d'autres types de fichiers sur le commutateur à partir d'un serveur de fichiers via une session TFTP, SFTP, SCP ou FTP, à partir d'un ordinateur via une session HTTP ou à partir d'un périphérique de stockage USB.

Vous pouvez vérifier manuellement la dernière version du logiciel (également appelée version du micrologiciel), télécharger le micrologiciel sur un serveur ou un ordinateur, puis télécharger le micrologiciel sur le commutateur. Si les notes de version du micrologiciel sont disponibles avec le nouveau micrologiciel, lisez-les pour savoir si vous devez reconfigurer le commutateur après la mise à jour.

Dans ce contexte, le téléchargement est également appelé mise à niveau.

Notez ce qui suit à propos des fichiers SSH et SSL :

- SSH Pour que vous puissiez télécharger des fichiers SSH sur le commutateur, SSH doit être désactivé administrativement et aucune session SSH active ne doit avoir lieu.
- SSL Les fichiers SSL contiennent des informations pour crypter, authentifier et valider les sessions HTTPS. Pour que vous puissiez télécharger des fichiers SSL sur le commutateur, HTTPS doit être désactivé administrativement.

Télécharger un fichier logiciel ou un autre type de fichier d'un serveur vers le commutateur

Vous pouvez télécharger une image logicielle (micrologiciel) et une configuration, SSL, PEM ou d'autres types de fichiers à partir d'un serveur TFTP, SFTP, SCP ou FTP de votre réseau vers le commutateur.

Avant de télécharger un fichier sur le commutateur, les conditions suivantes doivent être remplies :

- Le fichier à télécharger à partir du serveur se trouve sur le serveur dans le répertoire approprié.
- Le format du fichier est correct.
- Le commutateur contient un chemin d'accès au serveur.

Pour télécharger un fichier d'un serveur vers le commutateur :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **maintenance > mise à niveau > mise à niveau de fichier**.

La page File Upgrade s'affiche.

6. Dans le menu **type de fichier**, sélectionnez le type de fichier :

- **Logiciel** : L'image du logiciel système, qui est enregistrée dans l'un des deux secteurs Flash appelés images (image1 et image2). L'image active stocke la copie active, tandis que l'autre image stocke une seconde copie. Le périphérique démarre et s'exécute à partir de l'image active. Si l'image active est endommagée, le système démarre automatiquement à partir de l'image inactive. Il s'agit d'une fonction de sécurité pour les erreurs survenant pendant le processus de mise à niveau de l'amorçage. Il s'agit de l'option par défaut.
- **Configuration du texte** : Un fichier de configuration basé sur du texte vous permet de modifier un fichier texte configuré (**startup-config**) hors ligne selon vos besoins. L'utilisation la plus courante de la configuration textuelle est de télécharger une configuration de travail à partir d'un périphérique, de la modifier hors ligne pour la personnaliser pour un autre périphérique similaire (par exemple, changer le nom du périphérique ou l'adresse IP), et de la télécharger sur ce périphérique.
- **Fichier PEM de clé RSA SSH-2** : Un fichier de clé SSH-2 Rivest-Shamir-Adelman (RSA) (codé PEM).
- **Fichier PEM de clé DSA SSH-2** : Un fichier de clé SSH-2 Digital signature Algorithm (DSA) (codé PEM).
- **Fichier PEM de clé ECDSA** : Fichier de clé ECDSA (Elliptic Curve Digital signature Algorithm) (codé PEM).
- **Fichier PEM de certificat racine sécurisé SSL** : Un fichier de certificat racine sécurisé SSL (codé PEM).
- **Fichier PEM de certificat de serveur SSL** : Un fichier de certificat de serveur SSL (codé PEM) vers le terminal.

- **SSL DH 1024 fichier PEM de paramètre de cryptage** : Un fichier SSL Diffie-Hellman 1024 bits Encryption Parameter File (codé PEM) vers le périphérique.
 - **SSL DH 2048 fichier PEM de paramètre de cryptage** : Un fichier SSL Diffie-Hellman 2048 bits Encryption Parameter File (codé PEM) vers le périphérique.
 - **Fichier script** : Fichier de script de configuration texte. Vous devez utiliser l'interface de ligne de commande (CLI) pour configurer, valider et activer le script.
 - **Bannière CLI** : La bannière CLI contient le texte à afficher sur la CLI avant l'invite de connexion.
 - **Utilisateurs IAS** : Le fichier de base de données des utilisateurs du serveur d'authentification interne (IAS). La base de données des utilisateurs IAS stocke une liste de valeurs de nom d'utilisateur et de mot de passe (facultatif) pour l'authentification utilisateur locale basée sur le port.
 - **Configuration usine par défaut** : Le fichier de configuration usine par défaut est un fichier texte contenant la configuration usine par défaut enregistrée.
 - **Configuration de la clé publique** : Fichier de clé publique utilisé pour la validation du script de configuration.
 - **Application**. Fichiers d'une application.
 - **Fichier de commandes du support technique** : Un fichier contenant des commandes de support technique.
 - **Fichier de configuration du client DHCP** : Le fichier de configuration du client DHCP avec les informations du serveur DHCP (hôte).
7. Si la sélection dans le menu **type de fichier** est **logiciel**, le menu nom de l'image s'affiche et vous devez sélectionner l'image logicielle à télécharger sur le commutateur :
- Image1 : Sélectionnez image1 pour télécharger image1.
 - Image2 : Sélectionnez image2 pour télécharger image2.
- Nous vous recommandons de ne pas écraser l'image active.
8. Si la sélection dans le menu **type de fichier** est **logiciel**, les boutons radio vérifier s'affichent pour vous permettre de sélectionner l'une des options suivantes :
- **Aucun** : La vérification du fichier téléchargé est désactivée. Il s'agit de l'option par défaut.
 - **Vérifier** La signature numérique du fichier téléchargé est vérifiée.
 - **Pas de vérification**: La signature numérique du fichier téléchargé n'est pas vérifiée.

9. Si la sélection dans le menu **type de fichier** est **application**, le champ **nom du fichier d'application** s'affiche et vous devez spécifier le nom du fichier d'application.
10. Dans le menu **Transfer mode**, spécifiez le protocole à utiliser pour transférer le fichier vers le serveur :
 - TFTP Protocole Trivial File Transfer.
 - SFTP Protocole de transfert de fichiers sécurisé. Cette sélection nécessite la spécification d'un nom d'utilisateur et d'un mot de passe.
 - **SCP**: Protocole de copie sécurisé. Cette sélection nécessite la spécification d'un nom d'utilisateur et d'un mot de passe.
 - **FTP**. Protocole de transfert de fichiers. Cette sélection nécessite la spécification d'un nom d'utilisateur et d'un mot de passe.
11. Dans le menu **type d'adresse du serveur**, sélectionnez le format du champ **adresse du serveur** :
 - IPv4 : Indique que l'adresse du serveur est une adresse IPv4 au format décimal à points. Il s'agit de l'option par défaut.
 - IPv6 : Indique que l'adresse du serveur est une adresse IPv6 en nombres hexadécimaux utilisant des valeurs de 16 bits entre deux-points.
 - DNS : Indique que l'adresse du serveur est un nom d'hôte.
12. Dans le champ **adresse du serveur**, entrez l'adresse IP du serveur conformément au format indiqué par le type d'adresse du serveur.
L'adresse par défaut est l'adresse IPv4 0,0.0,0.
13. Dans le champ **chemin du fichier distant**, spécifiez le chemin sur le serveur où se trouve le fichier.
Le nom du chemin peut inclure uniquement des caractères alphabétiques, numériques, barre oblique, point ou trait de soulignement. Vous pouvez entrer jusqu'à 160 caractères.
14. Dans le champ **nom du fichier distant**, spécifiez le nom du fichier à télécharger.
Vous pouvez entrer jusqu'à 32 caractères.
15. Si vous sélectionnez **SFTP**, **SCP** ou **FTP** dans le menu **Transfer mode**, spécifiez les paramètres suivants :
 - Nom d'utilisateur : Spécifiez le nom d'utilisateur pour la connexion à distance au serveur.
 - Nouveau mot de passe : Spécifiez le mot de passe pour la connexion à distance au serveur.
16. Cliquez sur le bouton **Apply** (Appliquer).

Le fichier est téléchargé du serveur vers le commutateur. La page affiche des informations sur la progression du transfert de fichier.

17. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Utilisez HTTP pour télécharger un fichier logiciel ou un autre type de fichier sur le commutateur

Vous pouvez télécharger des fichiers de différents types depuis un ordinateur vers le commutateur via une session HTTP sur votre navigateur Web.

Pour utiliser HTTP pour télécharger un fichier d'un ordinateur vers le commutateur :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **maintenance > mise à niveau > mise à niveau du fichier HTTP** .

La page HTTP File Upgrade s'affiche.

6. Dans le menu **type de fichier**, sélectionnez le type de fichier :

- **Logiciel** : L'image du logiciel système, qui est enregistrée dans l'un des deux secteurs Flash appelés images (image1 et image2). L'image active stocke la copie active, tandis que l'autre image stocke une seconde copie. Le périphérique démarre et s'exécute à partir de l'image active. Si l'image active est endommagée, le système démarre automatiquement à partir de l'image inactive. Il s'agit d'une fonction de sécurité pour les erreurs survenant pendant le processus de mise à niveau de l'amorçage. Il s'agit de l'option par défaut.
- **Configuration du texte** : Un fichier de configuration basé sur du texte vous permet de modifier un fichier texte configuré (**startup-config**) hors ligne selon vos besoins. L'utilisation la plus courante de la configuration textuelle est de télécharger une configuration de travail à partir d'un périphérique, de la modifier hors ligne pour la personnaliser pour un autre périphérique similaire (par exemple, changer le nom du périphérique ou l'adresse IP), et de la télécharger sur ce périphérique.
- **Fichier PEM de clé RSA SSH-2** : Un fichier de clé SSH-2 Rivest-Shamir-Adelman (RSA) (codé PEM).
- **Fichier PEM de clé DSA SSH-2** : Un fichier de clé SSH-2 Digital signature Algorithm (DSA) (codé PEM).
- **Fichier PEM de clé ECDSA** : Fichier de clé ECDSA (Elliptic Curve Digital signature Algorithm) (codé PEM).
- **Fichier PEM de certificat racine sécurisé SSL** : Un fichier de certificat racine sécurisé SSL (codé PEM).
- **Fichier PEM de certificat de serveur SSL** : Un fichier de certificat de serveur SSL (codé PEM) vers le terminal.
- **SSL DH 1024 fichier PEM de paramètre de cryptage** : Un fichier SSL Diffie-Hellman 1048 bits Encryption Parameter File (codé PEM) vers le périphérique.
- **SSL DH 2048 fichier PEM de paramètre de cryptage** : Un fichier SSL Diffie-Hellman 2048 bits Encryption Parameter File (codé PEM) vers le périphérique.
- **Script de configuration** : Fichier de script de configuration texte. Vous devez utiliser l'interface de ligne de commande (CLI) pour configurer, valider et activer le script.
- **Bannière CLI** : La bannière CLI contient le texte à afficher sur la CLI avant l'invite de connexion.

- **Utilisateurs IAS** : Le fichier de base de données des utilisateurs du serveur d'authentification interne (IAS). La base de données des utilisateurs IAS stocke une liste de valeurs de nom d'utilisateur et de mot de passe (facultatif) pour l'authentification utilisateur locale basée sur le port.
 - **Configuration usine par défaut** : Le fichier de configuration usine par défaut est un fichier texte contenant la configuration usine par défaut enregistrée.
 - **Image clé publique** : Fichier de clé publique utilisé pour la validation de l'image de code.
 - **Fichier de configuration du client DHCP** : Le fichier de configuration du client DHCP avec les informations du serveur DHCP (hôte).
7. Si la sélection dans le menu **type de fichier** est **logiciel**, le menu **nom de l'image** s'affiche et vous devez sélectionner l'image logicielle à télécharger sur le commutateur :
- Image1 : Sélectionnez image1 pour télécharger image1.
 - Image2 : Sélectionnez image2 pour télécharger image2.
- Nous vous recommandons de ne pas écraser l'image active.
8. Si la sélection dans le menu **type de fichier** est **logiciel**, les boutons radio vérifier s'affichent pour vous permettre de sélectionner l'une des options suivantes :
- Aucun : La vérification du fichier téléchargé est désactivée. Il s'agit de l'option par défaut.
 - Vérifier La signature numérique du fichier téléchargé est vérifiée.
 - **Pas de vérification**: La signature numérique du fichier téléchargé n'est pas vérifiée.
9. En regard de sélectionner un fichier, cliquez sur le bouton **Parcourir**, naviguez jusqu'au fichier et sélectionnez le fichier à télécharger.
- Vous pouvez sélectionner un fichier dont le nom peut contenir jusqu'à 80 caractères.
10. Cliquez sur le bouton **Apply** (Appliquer).
- Le téléchargement commence.
- Le champ État du téléchargement affiche l'état pendant le transfert du fichier vers le commutateur.
- ❗ **Remarque**: Après le début du transfert de fichier, attendez que la page soit actualisée. Lorsque la page est actualisée, l'option sélectionner un fichier est vide, indiquant que le transfert de fichier est terminé.
11. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Télécharger un fichier logiciel ou un autre type de fichier d'un serveur vers le commutateur

Vous pouvez télécharger un fichier logiciel, un fichier de configuration texte ou un fichier de configuration client DHCP à partir d'un périphérique de stockage USB vers le commutateur.

Pour télécharger un fichier d'un périphérique de stockage USB vers le commutateur :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **maintenance > mise à niveau > mise à niveau du fichier USB**.

La page USB File Upgrade s'affiche.

6. Dans le menu **type de fichier**, sélectionnez le type de fichier à exporter :

- **Logiciel** : L'image du logiciel système, qui est enregistrée dans l'un des deux secteurs Flash appelés images (image1 et image2). L'image active stocke la copie active, tandis que l'autre image stocke une seconde copie. Le périphérique démarre et s'exécute à partir de l'image active. Si l'image active est endommagée, le système démarre automatiquement à partir de l'image inactive. Il s'agit d'une fonction de sécurité pour les erreurs survenant pendant le processus de mise à niveau de l'amorçage. Il s'agit de l'option par défaut.
 - **Configuration du texte** : Un fichier de configuration basé sur du texte vous permet de modifier un fichier texte configuré (**startup-config**) hors ligne selon vos besoins. L'utilisation la plus courante de la configuration textuelle est de télécharger une configuration de travail à partir d'un périphérique, de la modifier hors ligne pour la personnaliser pour un autre périphérique similaire (par exemple, changer le nom du périphérique ou l'adresse IP), et de la télécharger sur ce périphérique. Il s'agit de l'option par défaut.
 - **Fichier de configuration du client DHCP** : Le fichier de configuration du client DHCP avec les informations du serveur DHCP (hôte).
7. Si la sélection dans le menu **type de fichier** est **logiciel**, le menu **nom de l'image** s'affiche et vous devez sélectionner l'image logicielle à télécharger sur le commutateur :
- Image1 : Sélectionnez image1 pour télécharger image1.
 - Image2 : Sélectionnez image2 pour télécharger image2.
- Nous vous recommandons de ne pas écraser l'image active.
8. Si la sélection dans le menu **type de fichier** est **logiciel**, les boutons radio vérifier s'affichent pour vous permettre de sélectionner l'une des options suivantes :
- **Aucun** : La vérification du fichier téléchargé est désactivée. Il s'agit de l'option par défaut.
 - **Vérifier** La signature numérique du fichier téléchargé est vérifiée.
 - **Pas de vérification**: La signature numérique du fichier téléchargé n'est pas vérifiée.
9. Dans le champ **chemin du fichier**, spécifiez le chemin sur le périphérique de stockage USB.
- Vous pouvez entrer jusqu'à 146 caractères. La valeur par défaut est vide.
10. Dans le champ **fichier USB**, spécifiez le nom du fichier sur le périphérique de stockage USB.
- Vous pouvez entrer jusqu'à 32 caractères.
11. Cliquez sur le bouton **Apply** (Appliquer).

Le fichier est téléchargé du périphérique de stockage USB vers le commutateur. La page affiche des informations sur la progression du transfert de fichier.

12. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Téléchargez et installez un fichier de certificat de sécurité SSL sur le commutateur

Si vous utilisez HTTPS au lieu de HTTP pour accéder à l'interface utilisateur principale, vous n'avez pas besoin d'obtenir de certificat SSL. L'avertissement de sécurité qui peut s'afficher dans votre navigateur vous invite à confirmer que le certificat auto-signé du commutateur est valide. Une fois que vous l'avez fait, l'avertissement du navigateur peut ne plus s'afficher lorsque vous vous connectez.

Toutefois, si vous obtenez un certificat de sécurité SSL auprès d'une autorité de certification, vous pouvez télécharger et installer le certificat de sécurité SSL via une session HTTP à l'aide de votre navigateur Web.

Pour obtenir un certificat de sécurité SSL, vous devez télécharger deux fichiers PEM (Privacy Enhanced mail) sur le commutateur :

- **Fichier PEM de certificat racine sécurisé SSL** : Le fichier PEM du certificat racine de confiance SSL, qui doit être au format `xxxxCERTxxxxx.pem`.
- **Fichier PEM de certificat de serveur SSL** : Le fichier PEM du certificat de serveur SSL (le fichier de clé), qui doit être au format `xxxxKEYxxxxx.pem`.

Avant de pouvoir télécharger et installer un certificat de sécurité SSL, vous devez désactiver HTTPS sur le commutateur.

Pour désactiver HTTPS et utiliser une session HTTP pour télécharger et installer un fichier de certificat de sécurité SSL sur le commutateur :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **sécurité > accès > HTTPS > Configuration HTTPS**.

L'écran HTTPS Configuration (Configuration IP) s'affiche.

6. Sélectionnez le bouton radio **désactiver** le mode Admin.

7. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés. Comme vous avez changé le mode d'accès de HTTPS à HTTP, vous êtes déconnecté du commutateur.

8. Patientez une minute, actualisez votre navigateur et reconnectez-vous au commutateur.

9. Sélectionnez **maintenance > mise à niveau > mise à niveau du fichier HTTP**.

La page HTTP Firmware/File Update s'affiche.

10. Dans le menu **type de fichier**, sélectionnez **fichier PEM du certificat racine approuvé SSL**.

11. Sélectionnez le bouton sélectionner **Parcourir** le fichier et recherchez le fichier que vous souhaitez télécharger.

Il s'agit du fichier de certificat, qui doit être au format xxxxCERTxxxxx.pem.

12. Cliquez sur le bouton **Apply** (Appliquer).

Le transfert de fichier commence.

La page affiche des informations sur la progression du transfert de fichier. La page est actualisée automatiquement lorsque le transfert de fichier est terminé (ou si informatique échoue).

13. Dans le menu **type de fichier**, sélectionnez **certificat de serveur SSL fichier PEM**.

Il s'agit du fichier de clé, qui doit être au format xxxxKEYxxxxx.pem.

14. Sélectionnez le bouton sélectionner **Parcourir** le fichier et recherchez le fichier que vous souhaitez télécharger.

Le nom de fichier peut contenir jusqu'à 80 caractères.

15. Cliquez sur le bouton **Apply** (Appliquer).

Le transfert de fichier commence.

La page affiche des informations sur la progression du transfert de fichier. La page est actualisée automatiquement lorsque le transfert de fichier est terminé.

16. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Gérer les images logicielles .

Le commutateur conserve deux versions du logiciel du commutateur en stockage permanent. Une image est l'image active et la seconde image est l'image de sauvegarde. L'image active est chargée lorsque le commutateur démarre ou redémarre. Cette fonction réduit le temps d'arrêt du commutateur lorsque vous mettez à niveau le logiciel du commutateur.

Copier une image logicielle.

Vous pouvez copier une image logicielle d'un emplacement (principal ou de sauvegarde) à un autre.

Pour copier une image logicielle :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **maintenance > gestion des images > Copier**.

La page Copier s'affiche.

6. Sélectionnez le bouton radio image source **Image1** ou **Image2** pour spécifier l'image à copier.

7. Si le commutateur fait partie d'une pile, dans le menu **membre de pile**, sélectionnez le commutateur vers lequel l'image doit être copiée ou sélectionnez **tout** pour copier l'image sur tous les commutateurs.

Si votre commutateur ne fonctionne pas dans une pile, sélectionnez **1**.

8. Sélectionnez le bouton radio image de destination **Image1** ou **Image2** pour spécifier l'image de destination.

9. Cliquez sur le bouton **Apply** (Appliquer).

L'image est copiée.

10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Configurer les paramètres de double image

.

La fonction double image permet au commutateur de conserver deux images du micrologiciel dans un stockage permanent. Vous pouvez sélectionner l'image à charger lorsque le système redémarre, spécifier une description d'image ou supprimer une image. Cette fonction réduit le temps d'arrêt du commutateur lorsque vous mettez à niveau ou rétrogradez l'image logicielle.

Modifiez l'image logicielle qui se charge lorsque le commutateur démarre ou redémarre

Vous pouvez modifier l'image logicielle qui se charge lorsque le commutateur démarre. Si vous avez configuré une pile de commutateurs, vous pouvez sélectionner l'image qui se charge pour chaque commutateur de la pile.

Pour modifier l'image qui se charge pendant le processus de démarrage :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis.

Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **maintenance > gestion des images > Configuration image double**

.

La page Configuration d'image double s'affiche.

6. Cochez la case de l'image qui *n'est pas* l'image active (c'est-à-dire l'image pour laquelle les champs image active affichent faux) mais que vous souhaitez que le commutateur s'exécute *après* le redémarrage de informatique.

Si vous avez configuré une pile de commutateurs, vous pouvez sélectionner l'image qui se charge pour chaque commutateur de la pile.

7. Dans le menu **image active suivante**, sélectionnez **vrai**.
8. Vous pouvez également spécifier un nom pour l'image sélectionnée en le saisissant dans le champ **Description de l'image**.
9. Cliquez sur le bouton **Apply** (Appliquer).
Les paramètres sont enregistrés.
10. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.
11. Après avoir activé l'image, redémarrez le commutateur (voir [Redémarrez le commutateur à partir de l'interface utilisateur principale](#) à la page 1142).
Si vous ne redémarrez pas le commutateur, informatique continue à exécuter l'image affichée dans le champ actif courant jusqu'au prochain redémarrage du commutateur.

Le tableau suivant décrit les champs en lecture seule de la page.

Table 195 : Informations sur la configuration des images doubles

Champ	Description
Unité	ID de l'unité de pile de commutateurs. Si vous n'avez pas configuré de pile, l>ID de l'unité est 1.
Nom de l'image	Nom de l'image. Par défaut, les noms d'image sont image1 et image2.
Image active	Image active actuelle (vrai ou faux).
Version	Version du micrologiciel de l'image.

Supprimer une image logicielle

Vous pouvez supprimer une image logicielle qui n'est pas l'image active. Si vous avez configuré une pile de commutateurs, vous pouvez supprimer l'image qui n'est pas l'image active pour un ou plusieurs commutateurs de la pile.

Pour supprimer une image logicielle :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **maintenance > gestion des images > Configuration image double**

La page Configuration d'image double s'affiche.

6. Cochez la case de l'image qui *n'est pas* l'image active (c'est-à-dire l'image pour laquelle les champs image active affichent faux).

Si vous avez configuré une pile de commutateurs, vous pouvez sélectionner l'image d'un ou plusieurs commutateurs de la pile.

Vous ne pouvez pas supprimer l'image active. Pour l'image active actuelle, le champ image active affiche vrai.

7. Cliquez sur le bouton **Supprimer**.

L'image est supprimée.

8. Pour enregistrer les paramètres dans la configuration en cours, cliquez sur l'icône **Enregistrer**.

Diagnostique et dépannage

Vous pouvez envoyer un ping, tracer une route et effectuer un vidage de mémoire.

Envoyez une requête ping à une adresse IPv4.

Vous pouvez configurer le commutateur pour envoyer une requête ping à une adresse IPv4 spécifiée. Vous pouvez utiliser cette option pour vérifier si le commutateur peut

communiquer avec un périphérique IPv4 particulier. Lorsque vous envoyez une requête ping, le commutateur envoie un nombre spécifié de requêtes ping et les résultats sont affichés.

Si une réponse au ping est reçue, le message suivant s'affiche :

```
PING x.y.z.w (x.y.z.w) : taille des octets de données
```

```
taille octets de x.y.z.w : seq=0 ttl=xyz
```

```
--- x.y.z.w statistiques ping ---
```

```
comptage des paquets transmis, comptage des paquets reçus, x % de perte de paquets
```

Si aucune réponse au ping n'est reçue, le message suivant s'affiche :

```
PING x.y.z.w (x.y.z.w) : taille des octets de données
```

```
--- x.y.z.w statistiques ping ---
```

```
nombre de paquets transmis, 0 paquets reçus, perte de paquets de 100%
```

Pour envoyer une requête ping à une adresse IPv4 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **maintenance > Dépannage > Ping IPv4**.

La page Ping IPv4 s'affiche.

6. Dans le champ **adresse IP/nom d'hôte**, entrez l'adresse IP ou le nom d'hôte du périphérique qui doit être soumis à la commande ping.

Le format est x.x.x.x. Le nombre maximum de caractères est de 255.

7. Dans le champ **nombre**, entrez le nombre de demandes d'écho qui doivent être envoyées.

La valeur par défaut est 3. La plage est de 1 à 15.

8. Dans le champ **intervalle (sec)**, entrez le temps entre les paquets ping en secondes.

La valeur par défaut est 3 secondes. La plage est de 1 à 60.

9. Dans le champ **taille du datagramme**, entrez la taille du paquet ping.

La valeur par défaut est 0 octet. La plage est de 0 à 13000.

10. Dans le menu **source**, vous pouvez sélectionner en option l'adresse IP ou l'interface qui doit être utilisée pour envoyer des paquets de requête d'écho :

- **Aucun** : L'adresse source du paquet ping est l'adresse de l'interface de sortie par défaut.
- **IP Address** (Adresse IP). Adresse IP source qui doit être utilisée lors de l'envoi de paquets de demande d'écho. Avec cette sélection, le champ **adresse IP** s'affiche et vous devez saisir l'adresse IPv4 qui doit être utilisée comme source.
- **Interface** Interface qui doit être utilisée lorsque des paquets de requête d'écho sont envoyés. Le menu **interface** s'affiche et vous devez sélectionner l'interface.

11. Cliquez sur le bouton **Apply** (Appliquer).

L'adresse spécifiée fait l'objet d'un ping. Les résultats sont affichés sous les données configurables dans le champ résultats.

Envoyez une requête ping à une adresse IPv6.

Vous pouvez configurer le commutateur pour envoyer une requête ping à une adresse IPv6 spécifiée. Vous pouvez utiliser cette option pour vérifier si le commutateur peut communiquer avec un périphérique IPv6 particulier. Lorsque vous envoyez une requête ping, le commutateur envoie un nombre spécifié de requêtes ping et les résultats sont affichés.

Si une réponse au ping est reçue, le message suivant s'affiche :

```
PING x:y ::z:w (x:y ::z:w) : taille des octets de données
```

```
taille octets de x:y ::z:w : seq=0 ttl=xyz
```

```
--- x:y ::z:w statistiques ping ---
```

```
comptage des paquets transmis, comptage des paquets reçus, x % de perte de paquets
```

Si aucune réponse au ping n'est reçue, le message suivant s'affiche :

```
PING x:y ::z:w (x:y ::z:w) : taille des octets de données
```

```
--- x:y ::z:w statistiques ping ---
```

```
nombre de paquets transmis, 0 paquets reçus, perte de paquets de 100%
```

Pour envoyer une requête ping à une adresse IPv6 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :
Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.
La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.
La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **maintenance > Dépannage > Ping IPv6**.

La page Ping IPv6 s'affiche.

6. Dans le menu **Ping**, sélectionnez le type de ping :

- **Global** : Envoie une requête ping à une adresse IPv6 globale.
- **Lien local** : Envoie une requête ping à une adresse IPv6 lien-local sur une interface spécifiée. Lorsque vous sélectionnez cette option, le menu **interface** s'affiche et vous devez sélectionner l'interface.

7. Dans le champ **adresse IPv6/nom d'hôte**, entrez l'adresse IPv6 ou le nom d'hôte de la station qui doit faire l'objet d'un ping.

Le format est xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx. Le nombre maximum de caractères est de 255.

8. Dans le champ **nombre**, entrez le nombre de demandes d'écho qui doivent être envoyées.

La plage est de 1 à 15. La valeur par défaut est 3.

9. Dans le champ **intervalle (sec)**, entrez le temps en secondes entre les paquets ping.

La plage est de 1 à 60. La valeur par défaut est 3.

10. Dans le champ **taille du datagramme**, entrez la taille du datagramme.

La plage valide est comprise entre 0 et 13000 caractères. La valeur par défaut est 0 octet.

11. Dans le menu **source**, vous pouvez sélectionner en option l'adresse IP ou l'interface qui doit être utilisée pour envoyer des paquets de requête d'écho :

- Aucun : L'adresse source du paquet ping est l'adresse de l'interface de sortie par défaut.
- Adresse IPv6 : Adresse IP source qui doit être utilisée lors de l'envoi de paquets de demande d'écho. Avec cette sélection, le champ **adresse IPv6** s'affiche et vous devez entrer l'adresse IPv6 qui doit être utilisée comme source.
- Interface Interface qui doit être utilisée lorsque des paquets de requête d'écho sont envoyés. Le menu **interface** s'affiche et vous devez sélectionner l'interface.

12. Cliquez sur le bouton **Apply** (Appliquer).

L'adresse spécifiée fait l'objet d'un ping. Les résultats sont affichés sous les données configurables dans le champ résultats.

Envoyer un traceroute IPv4.

Vous pouvez configurer le commutateur pour envoyer une requête traceroute à une adresse IPv4 ou un nom d'hôte spécifié. Vous pouvez l'utiliser pour découvrir les chemins empruntés par les paquets vers une destination distante. Lorsque vous envoyez un traceroute, le commutateur affiche les résultats sous les données configurables.

Si une réponse au traceroute est reçue, le message suivant s'affiche :

```
Traceroute vers x.y.z.w (x.y.z.w), maxTTL sauts max, taille des paquets en octets
```

```
InitTTL x.y.z.w (x.y.z.w) 0,000 ms * 0,000 ms.
```

```
InitTTL+1 x.y.z.w (x.y.z.w) 0,000 ms * 0,000 ms.
```

```
InitTTL+2 x.y.z.w (x.y.z.w) 0,000 ms * 0,000 ms.
```

Pour envoyer un traceroute IPv4 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **maintenance > Dépannage > Traceroute IPv4**.

La page Traceroute IPv4 s'affiche.

6. Dans le champ **adresse IP/nom d'hôte**, entrez l'adresse IP ou le nom d'hôte du périphérique pour lequel le chemin doit être découvert.

7. Dans le champ **sondes par saut**, saisissez le nombre de sondes par saut.

La valeur par défaut est 3. La plage est de 1 à 10.

8. Dans le champ **TTL max.**, entrez la durée de vie maximale (TTL) pour la destination.

La valeur par défaut est 30. La plage est de 1 à 255.

9. Dans le champ **Init TTL**, entrez le TTL initial à utiliser.

La valeur par défaut est 1. La plage est de 1 à 255.

10. Dans le champ **MaxFail**, entrez le nombre maximal d'échecs autorisés dans la session.

La valeur par défaut est 5. La plage est de 1 à 255.

11. Dans le champ **intervalle (s)**, entrez le temps entre les sondes en secondes.

La valeur par défaut est 3. La plage est de 1 à 60.

12. Dans le champ **Port**, entrez le port de destination UDP pour les paquets de test.

La valeur par défaut est 33434. La plage est de 1 à 65535.

13. Dans le champ **taille**, entrez la taille des paquets de test.

La valeur par défaut est 0. La plage est de 0 à 39936.

14. Dans le menu **source**, vous pouvez sélectionner en option l'adresse IP ou l'interface à utiliser pour envoyer des paquets de test :

- Aucun : L'adresse source du paquet sonde est l'adresse de l'interface de sortie par défaut.
- **IP Address** (Adresse IP). Adresse IP source qui doit être utilisée lors de l'envoi de paquets de requête d'exploration. Avec cette sélection, le champ **adresse IP** s'affiche et vous devez saisir l'adresse IPv4 qui doit être utilisée comme source.
- Interface Interface qui doit être utilisée lors de l'envoi de paquets de requête de sonde. Le menu **interface** s'affiche, mais la seule option disponible dans le menu est **réseau**.

15. Cliquez sur le bouton **Apply** (Appliquer).

Une requête traceroute est envoyée à l'adresse IP ou au nom d'hôte spécifié. Les résultats sont affichés sous les données configurables dans le champ résultats.

Envoyer un traceroute IPv6.

Vous pouvez configurer le commutateur pour envoyer une requête traceroute à une adresse IPv6 ou un nom d'hôte spécifié. Vous pouvez l'utiliser pour découvrir les chemins empruntés par les paquets vers une destination distante. Lorsque vous envoyez un traceroute, le commutateur affiche les résultats sous les données configurables.

Si une réponse au traceroute est reçue, le message suivant s'affiche :

```
Traceroute vers x:y ::z:w (x:y ::z:w), maxTTL sauts max, taille des paquets en octets
```

```
InitTTL x:y ::z:w (x:y ::z:w) 0,000 ms * 0,000 ms.
```

```
InitTTL+1 x:y ::z:w (x:y ::z:w) 0,000 ms * 0,000 ms.
```

```
InitTTL+2 x:y ::z:w (x:y ::z:w) 0,000 ms * 0,000 ms.
```

Pour envoyer un traceroute IPv6 :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.
La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.
- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)
La page System Information (Informations système) s'affiche.
5. Sélectionnez **maintenance > Dépannage > Traceroute IPv6**.
La page Traceroute IPv6 s'affiche.
6. Dans le champ **adresse IPv6/nom d'hôte**, entrez l'adresse IPv6 ou le nom d'hôte du périphérique pour lequel le chemin doit être découvert.
7. Dans le champ **sondes par saut**, saisissez le nombre de sondes par saut.
La valeur par défaut est 3. La plage est de 1 à 10.
8. Dans le champ **TTL max.**, entrez la durée de vie maximale (TTL) pour la destination.
La valeur par défaut est 30. La plage est de 1 à 255.
9. Dans le champ **Init TTL**, entrez le TTL initial à utiliser.
La valeur par défaut est 1. La plage est de 1 à 255.
10. Dans le champ **MaxFail**, entrez le nombre maximal d'échecs autorisés dans la session.
La valeur par défaut est 5. La plage est de 1 à 255.
11. Dans le champ **intervalle (s)**, entrez le temps entre les sondes en secondes.
La valeur par défaut est 3. La plage est de 1 à 60.
12. Dans le champ **Port**, entrez le port de destination UDP pour les paquets de test.
La valeur par défaut est 33434. La plage est de 1 à 65535.
13. Dans le champ **taille**, entrez la taille des paquets de test.
La valeur par défaut est 0. La plage est de 0 à 39936.
14. Dans le menu **source**, vous pouvez sélectionner en option l'adresse IP ou l'interface à utiliser pour envoyer des paquets de test :

- Aucun : L'adresse source du paquet sonde est l'adresse de l'interface de sortie par défaut.
- Adresse IPv6 : Adresse IP source qui doit être utilisée lors de l'envoi de paquets de demande d'écho. Avec cette sélection, le champ **adresse IPv6** s'affiche et vous devez entrer l'adresse IPv6 qui doit être utilisée comme source.
- Interface Interface qui doit être utilisée lorsque des paquets de requête d'écho sont envoyés. Le menu interface s'affiche et vous devez sélectionner l'interface.

15. Cliquez sur le bouton **Apply** (Appliquer).

Une requête traceroute est envoyée à l'adresse IP ou au nom d'hôte spécifié. Les résultats sont affichés sous les données configurables dans le champ résultats.

Capturer des paquets

Vous pouvez capturer et stocker des paquets sur un périphérique de stockage USB.

Pour lancer la capture de paquets :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.

2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.

3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :

- Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur principale à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **maintenance > Dépannage > capture de paquets**.

La page Capture de paquets s'affiche.

6. En regard de RPCAP USB, sélectionnez le bouton radio **Activer**.
7. Dans le menu **mode de capture**, sélectionnez le type de trafic à capturer :
 - TOUT Capturez tout le trafic. Il s'agit de l'option par défaut.
 - **TX** : Capturez uniquement le trafic transmis.
 - **RX** : Capturer uniquement le trafic reçu.
8. Dans le champ **nom du fichier**, spécifiez le nom du fichier USB.

Le nom de fichier ne peut pas inclure les symboles suivants : ' \ : * ? " < > | ' . Vous pouvez spécifier jusqu'à 64 caractères, à l'exclusion de l'extension, qui est ajoutée automatiquement.
9. Pour démarrer le processus de capture de paquets, cliquez sur le bouton **Démarrer**.

Les paquets sont capturés jusqu'à ce que vous arrêtiez le processus.
10. Pour arrêter le processus de capture de paquets, procédez comme suit :
 - a. En regard de RPCAP USB, sélectionnez le bouton radio **désactiver**.
 - b. Cliquez sur le bouton **Apply** (Appliquer).

Le processus de capture de paquets s'arrête.

Effectuez un vidage mémoire complet

Vous pouvez effectuer un vidage mémoire complet pour récupérer le vidage mémoire à des fins de dépannage.

Pour effectuer un vidage mémoire complet :

1. Lancez un navigateur Web et saisissez l'adresse IP par défaut du switch dans la barre d'adresse du navigateur :

Si vous ne connaissez pas l'adresse IP du commutateur, reportez-vous à [Connectez-vous à l'interface utilisateur principale à l'aide d'un navigateur Web](#) à la page 33 la section et aux sous-sections.

La page de connexion s'affiche.
2. Cliquez sur le bouton **connexion à l'interface utilisateur principale**.

La page de connexion à l'interface principale s'affiche dans un nouvel onglet.
3. Entrez **admin** comme nom d'utilisateur et entrez l'un des mots de passe suivants :
 - Saisissez le nouveau mot de passe de votre appareil local.

La première fois que vous vous connectez, aucun mot de passe n'est requis. Cependant, vous devez ensuite spécifier un mot de passe de périphérique local à utiliser chaque fois que vous vous connectez.

- Si vous gérez le commutateur via le contrôleur d'engagement, saisissez le mot de passe du site d'engagement auquel le commutateur est intégré.
- Si, en plus de l'interface utilisateur AV, vous gérez également le commutateur via le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour le réseau Insight auquel le commutateur est ajouté.

Pour plus d'informations sur les paramètres, reportez-vous à la section [Informations d'identification de l'interface utilisateur principale](#) à la page 46.

4. Cliquez sur le bouton **Login** (Connexion)

La page System Information (Informations système) s'affiche.

5. Sélectionnez **maintenance > Dépannage > vidage mémoire pleine**.

La page vidage mémoire complet s'affiche.

6. Dans le menu **Protocole**, sélectionnez le protocole utilisé pour transférer le fichier de vidage principal :

- **Aucun** : La fonctionnalité de vidage de mémoire est désactivée.
- **TFTP** Les résultats sont transférés vers un serveur TFTP.
- **USB** Les résultats sont transférés vers un périphérique de stockage USB. Il s'agit de l'option par défaut.
- **FTP**. Les résultats sont transférés vers un serveur FTP.

7. Si vous sélectionnez **TFTP** ou **FTP** dans le menu **Protocole**, des champs supplémentaires s'affichent sur la page, vous permettant de spécifier les paramètres du serveur :

- **TFTP** Dans le champ **adresse du serveur**, spécifiez l'adresse IP du serveur TFTP.
- **FTP**. Spécifiez les paramètres de serveur suivants :
 - **Server Address** (Adresse du serveur). Spécifiez l'adresse IP du serveur FTP.
 - **Nom d'utilisateur** : Spécifiez le nom d'utilisateur pour la connexion à distance au serveur.
 - **Nouveau mot de passe** : Spécifiez le mot de passe pour la connexion à distance au serveur.

8. Dans le champ **chemin du fichier**, spécifiez le chemin d'accès à l'emplacement de stockage du fichier de vidage principal.

9. Dans le champ **nom du fichier**, spécifiez le nom du fichier de vidage principal.

Le nom par défaut est core.

10. Pour ajouter le nom d'hôte au nom du fichier de vidage principal, cochez la case **nom d'hôte**.

11. Pour ajouter un horodatage au nom du fichier de vidage principal, cochez la case **horodatage**.

Cette case à cocher est activée par défaut.

12. Pour vider le registre de puce de commutation en cas d'exception, cochez la case **vider le registre de commutation**.

13. Cochez l'une des cases suivantes :

- **Écrire le test de base** : Pour générer un vidage de mémoire de test mais ne pas transférer informatique vers le serveur ou le périphérique de stockage USB, cochez la case écrire un test de mémoire.
- **Écrire le noyau** : Pour générer un vidage mémoire et transférer informatique vers le serveur ou le périphérique de stockage USB, cochez la case écrire mémoire mémoire.

14. Si vous cochez la case **écrire noyau**, pour enregistrer les paramètres actuels, cochez la case **Enregistrer les paramètres** actuels.

Cette case à cocher est activée par défaut.

 **Attention:** Le commutateur redémarre lorsque vous cliquez sur le bouton **appliquer**.

15. Cliquez sur le bouton **Apply** (Appliquer).

Le vidage de mémoire est envoyé à l'emplacement spécifié. Le commutateur redémarre. Ce processus prend environ 135 secondes.

12

Exemples de configuration

Cette annexe contient des informations sur la configuration des fonctions suivantes :

- Réseaux locaux virtuels (VLAN).
- Listes de contrôle d'accès (ACL)
- Services différenciés (DiffServ).
- Contrôle d'accès au port 802.1X.
- Protocole Spanning Tree multiple.
- Interfaces de routage VLAN

Réseaux locaux virtuels (VLAN) .

Un réseau local (LAN) peut généralement être défini comme un domaine de diffusion. Les concentrateurs, ponts ou commutateurs situés dans le même segment physique ou les mêmes segments connectent tous les périphériques de nœud final. Les nœuds finaux peuvent communiquer entre eux sans avoir besoin d'un routeur. Les routeurs connectent les réseaux locaux entre eux et acheminent le trafic vers le port approprié.

Un réseau local virtuel (VLAN) est un réseau local avec une définition qui mappe les postes de travail sur une base autre que l'emplacement géographique (par exemple, par service, type d'utilisateur ou application principale). Pour permettre au trafic de circuler entre les VLAN, le trafic doit passer par un routeur, comme si les VLAN étaient sur deux LAN distincts.

Un VLAN est un groupe d'ordinateurs, de serveurs et d'autres ressources réseau qui se comportent comme s'ils étaient connectés à un seul segment de réseau, même s'ils ne l'étaient pas. Par exemple, tout le personnel marketing peut être réparti dans un bâtiment. Pourtant, s'ils sont tous affectés à un seul VLAN, ils peuvent partager les ressources et la bande passante comme s'ils étaient connectés au même segment. Les ressources des autres départements peuvent être invisibles pour les membres du VLAN marketing, accessibles à tous ou accessibles uniquement à des personnes spécifiées, selon la manière dont le gestionnaire informatique a configuré les VLAN.

Les VLAN présentent un certain nombre d'avantages :

- informatique est facile à faire de la segmentation de réseau. Les utilisateurs qui communiquent le plus fréquemment entre eux peuvent être regroupés dans des VLAN communs, quel que soit leur emplacement physique. Le trafic de chaque groupe est en grande partie contenu dans le VLAN, ce qui réduit le trafic superflu et améliore l'efficacité de l'ensemble du réseau.
- Ils sont faciles à gérer. L'ajout de nœuds, ainsi que les déplacements et autres modifications, peuvent être traités rapidement et facilement à partir d'une interface de gestion plutôt que depuis l'armoire de câblage.
- Ils offrent des performances accrues. Les VLAN libèrent de la bande passante en limitant le trafic nœud à nœud et broadcast sur l'ensemble du réseau.
- Ils garantissent une sécurité réseau renforcée. Les VLAN créent des limites virtuelles qui ne peuvent être franchies que par un routeur. Des mesures de sécurité standard basées sur les routeurs peuvent donc être utilisées pour restreindre l'accès à chaque VLAN.

Les paquets reçus par le commutateur sont traités de la manière suivante :

- Lorsqu'un paquet non étiqueté pénètre dans un port, informatique est automatiquement étiqueté avec le numéro d'étiquette VLAN ID par défaut du port. Chaque port prend en charge un paramètre d'ID VLAN par défaut configurable (le

paramètre par défaut est 1). Le paramètre VLAN ID par défaut de chaque port peut être modifié sur la page Configuration PVID du port. Consultez la section .

- Lorsqu'un paquet étiqueté pénètre dans un port, l'étiquette de ce paquet n'est pas affectée par le paramètre ID VLAN par défaut. Le paquet passe au VLAN spécifié par son numéro d'étiquette d'identification VLAN.
- Si le port par lequel le paquet entre n'est pas membre du VLAN comme spécifié par la balise d'ID VLAN, le paquet est abandonné.
- Si le port est membre du VLAN spécifié par l'ID VLAN du paquet, le paquet peut être envoyé à d'autres ports avec le même ID VLAN.
- Les paquets quittant le commutateur sont étiquetés (T) ou non étiquetés (U), selon le paramètre des propriétés d'appartenance VLAN de ce port. Un « U » pour un port signifie que les paquets quittant le commutateur à partir de ce port ne sont pas étiquetés. Un « T » pour un port signifie que les paquets quittant le commutateur à partir de ce port sont étiquetés avec l'ID VLAN associé au port.

L'exemple de cette section comprend de nombreuses étapes illustrant un large éventail de configurations afin de mieux comprendre les VLAN balisés.

Exemples de configuration VLAN.

Cet exemple illustre plusieurs scénarios d'utilisation de VLAN et décrit comment le commutateur gère le trafic balisé et non balisé.

Dans cet exemple, vous créez deux nouveaux VLAN, modifiez l'appartenance au port pour le VLAN 1 par défaut et affectez des membres de port aux deux nouveaux VLAN :

1. Dans la page Configuration VLAN de base (voir [VLAN](#) à la page 310), créez les VLAN suivants :
 - VLAN non étiqueté avec VLAN ID 10
 - VLAN non étiqueté avec VLAN ID 20
2. Sur la page adhésion à VLAN (voir [Configurer les interfaces d'appartenance pour un VLAN](#) à la page 322), spécifiez l'adhésion à VLAN comme suit :
 - Pour le VLAN par défaut avec ID VLAN 1, spécifiez les membres suivants : Port 7 (U) et Port 8 (U).
 - Pour le VLAN avec VLAN ID 10, spécifiez les membres suivants : port 1 (U), port 2 (U) et port 3 (T).
 - Pour le VLAN avec l'ID VLAN 20, spécifiez les membres suivants : port 4 (U), port 5 (T) et port 6 (U).

3. Sur la page Configuration PVID du port (voir [Modifiez les paramètres de l'ID VLAN du port](#) à la page 325), spécifiez le PVID des ports g1 et g4 afin que les paquets entrant dans ces ports soient balisés avec l'ID VLAN du port :
 - Port 1 : PVID 10
 - Port 4 : PVID 20
4. Avec la configuration VLAN que vous avez configurée, les situations suivantes produisent les résultats décrits ci-dessous :
 - Si un paquet non étiqueté entre dans le port 1, le commutateur étiquette informatique avec l'ID VLAN 10. Le paquet peut accéder au port 2 et au port 3. Le paquet sortant est retiré de son étiquette pour quitter le port 2 comme paquet non étiqueté. Pour le port 3, le paquet sortant part sous forme de paquet étiqueté avec l'ID VLAN 10.
 - Si un paquet étiqueté avec l'ID VLAN 10 entre dans le port 3, le paquet peut accéder au port 1 et au port 2. Si le paquet quitte le port 1 ou le port 2, informatique est dépouillé de son étiquette pour laisser le commutateur en tant que paquet non étiqueté.
 - Si un paquet non étiqueté entre dans le port 4, le commutateur étiquette informatique avec l'ID VLAN 20. Le paquet peut accéder au port 5 et au port 6. Le paquet sortant est retiré de son étiquette pour devenir un paquet non étiqueté lorsque informatique quitte le port 6. Pour le port 5, le paquet sortant part sous forme de paquet étiqueté avec l'ID VLAN 20.

Listes de contrôle d'accès (ACL)

Les listes de contrôle d'accès garantissent que seuls les utilisateurs autorisés peuvent accéder à des ressources spécifiques tout en bloquant toute tentative injustifiée d'atteindre des ressources réseau.

Les listes de contrôle d'accès sont utilisées pour contrôler le flux de trafic, restreindre le contenu des mises à jour de routage, décider quels types de trafic sont transférés ou bloqués et assurer la sécurité du réseau. Les listes de contrôle d'accès sont normalement utilisées dans les routeurs pare-feu placés entre le réseau interne et un réseau externe, tel qu'Internet. Ils peuvent également être utilisés sur un routeur positionné entre deux parties du réseau pour contrôler le trafic entrant ou sortant d'une partie spécifique du réseau interne. Le traitement des paquets ajouté requis par la fonction ACL n'affecte pas les performances du commutateur. C'est-à-dire que le traitement des listes de contrôle d'accès se produit à la vitesse du fil.

Les listes d'accès sont un ensemble séquentiel de conditions d'autorisation et de refus. Cet ensemble de conditions, appelé critères de filtrage, est appliqué à chaque paquet

traité par le commutateur ou le routeur. Le transfert ou l'abandon d'un paquet est basé sur le fait que le paquet correspond ou non aux critères spécifiés.

Le filtrage du trafic nécessite les deux étapes de base suivantes :

1. Créez une définition de liste d'accès.

La définition de liste d'accès comprend des règles qui spécifient si le trafic correspondant aux critères est transféré normalement ou rejeté. En outre, vous pouvez affecter le trafic correspondant aux critères à une file d'attente particulière ou rediriger le trafic vers un port particulier. Une règle *refuser tout* par défaut est la dernière règle de chaque liste.

2. Appliquez la liste d'accès à une interface dans la direction entrante.

Le commutateur permet aux ACL d'être liées aux ports physiques et aux LAG. Le commutateur prend en charge les ACL MAC et IP.

Exemple de configuration de l'ACL MAC

L'exemple suivant montre comment créer une liste de contrôle d'accès MAC qui autorise le trafic Ethernet du service commercial sur des ports spécifiés et refuse tout autre trafic sur ces ports.

1. Sur la page ACL MAC, créez une ACL nommée Sales_ACL pour le service commercial de votre réseau (voir [Configurez une ACL MAC](#) à la page 1036).

Par défaut, cette liste de contrôle d'accès est liée à la direction entrante, ce qui signifie que le commutateur examine le trafic lorsque informatique entre dans le port.

2. Sur la page règles MAC, créez une règle pour Sales_ACL avec les paramètres suivants :

- **Numéro de séquence** : 1
- Action : Permis
- **Attribuer un ID de file d'attente** : 0
- **Correspondre tous les** : Faux
- **Cos** : 0
- **MAC de destination** : 01 :02 :1A :BC :DE :SUP
- **Masque MAC de destination** : 00 :00 :00 :00 :FF :FF
- **EtherType** : Valeur utilisateur
- **Source MAC** (Adresse IP source). 02 :02 :1A :BC :DE :SUP
- **Masque MAC source** : 00 :00 :00 :00 :FF :FF
- Identifiant VLAN : 2

Pour plus d'informations sur les règles ACL MAC, reportez-vous à la section [Configurer les règles ACL MAC](#), à la page 1040.

3. Sur la page Configuration de la liaison MAC, affectez à Sales_ACL les valeurs 6, 7 et 8, puis cliquez sur le bouton **appliquer**. (Consultez la section [Configurer les liaisons MAC](#), à la page 1045.)

Vous pouvez attribuer un numéro de séquence facultatif pour indiquer l'ordre de cette liste d'accès par rapport aux autres listes d'accès si des listes d'accès sont déjà attribuées à cette interface et à cette direction.

4. Le tableau de liaison MAC affiche les informations de liaison de l'interface et de la liste de contrôle d'accès MAC. (Consultez la section [Affichez ou supprimez les liaisons MAC ACL dans la table de liaison MAC](#), à la page 1047.)

La liste de contrôle d'accès appelée Sales_ACL recherche les trames Ethernet avec les adresses MAC de destination et source et les masques MAC définis dans la règle. En outre, le cadre doit être étiqueté avec l'ID VLAN 2, qui est le VLAN du service commercial. La valeur cos de la trame doit être 0, qui est la valeur par défaut pour les trames Ethernet. Les trames qui correspondent à ces critères sont autorisées sur les interfaces 6, 7 et 8 et sont affectées à la file d'attente de sortie matérielle 0, qui est la file d'attente par défaut. Tout autre trafic est explicitement refusé sur ces interfaces. Pour autoriser le trafic supplémentaire à entrer dans ces ports, vous devez ajouter une nouvelle règle autoriser avec les critères de correspondance souhaités et lier la règle aux interfaces 6, 7 et 8.

Exemple de configuration de l'ACL IP de base

L'exemple suivant montre comment créer une liste de contrôle d'accès IP qui empêche tout trafic IP du service financier d'être autorisé sur les ports associés à d'autres services. Le trafic provenant du département Finance est identifié par l'adresse IP réseau de chaque paquet.

1. Sur la page IP ACL, créez une nouvelle ACL IP avec l'ID IP ACL 1. (Consultez la section [.](#))
2. Sur la page IP Rules, créez une règle pour IP ACL 1 avec les paramètres suivants :
 - **Numéro de séquence** : 1
 - Action : Refuser
 - **Attribuer un ID de file d'attente** : 0 (facultatif : 0 est la valeur par défaut)
 - **Correspondre tous les** : Faux

- Adresse IP source 192.168.187.0
- **Masque IP source** : 255.255.0

Pour plus d'informations sur les règles de liste de contrôle d'accès IP, reportez-vous à la section Configurer des règles pour une liste de contrôle d'accès IPv4 de base à la page 1053.

3. Cliquez sur le bouton **Add** (Ajouter).
 4. Sur la page IP Rules, créez une deuxième règle pour IP ACL 1 avec les paramètres suivants :
 - **Numéro de séquence** : 2
 - Action : Permis
 - **Correspondre tous les** : Vrai
 5. Cliquez sur le bouton **Add** (Ajouter).
 6. Sur la page Configuration de la liaison IP, attribuez l'ID ACL 1 aux ports 2, 3 et 4 et attribuez un numéro de séquence 1. (Consultez la section .)
- Par défaut, cette liste de contrôle d'accès IP est liée à la direction entrante, de sorte que informatique examine le trafic lorsque informatique entre dans le commutateur.
7. Cliquez sur le bouton **Apply** (Appliquer).
 8. Sur la page table de liaison IP, vous pouvez afficher les interfaces et les informations de liaison IP ACL. (Consultez la section .)

Dans cet exemple, la liste de contrôle d'accès IP fait correspondre tous les paquets avec l'adresse IP source et le masque de sous-réseau du réseau du service financier et Deny informatique sur les interfaces 2, 3 et 4 du commutateur. La deuxième règle autorise tout trafic non financier sur les ports. La deuxième règle est requise car une règle de *refus* explicite existe en tant que règle de priorité la plus basse.

Services différenciés (DiffServ) .

Les réseaux IP standard sont conçus pour fournir un service de livraison de données *optimal*. Le service *Best effort* implique que le réseau livre les données en temps opportun, même si rien ne garantit que informatique le fasse. Pendant les périodes de congestion, les paquets peuvent être retardés, envoyés sporadiquement ou abandonnés. Pour les applications Internet typiques, telles que le courrier électronique et le transfert de fichiers, une légère dégradation du service est acceptable et, dans de nombreux cas, invisible. Cependant, toute dégradation du service peut affecter négativement les applications nécessitant des délais stricts, telles que la voix ou le multimédia.

La qualité de service est un moyen d'obtenir une transmission de données prévisible et cohérente en distinguant les paquets dont les exigences temporelles sont strictes de ceux qui tolèrent plus facilement les retards. Les paquets avec des exigences de synchronisation strictes reçoivent un traitement spécial dans un réseau compatible QoS. Dans cet esprit, tous les éléments du réseau doivent être compatibles QoS. Si un nœud ne peut pas répondre aux exigences de synchronisation nécessaires, cela crée une déficience dans le chemin du réseau et les performances de l'ensemble du flux de paquets sont compromises.

Il existe deux types de QoS de base :

- **Services intégrés** : Les ressources du réseau sont réparties sur la base d'une demande et sont réservées (réservation de ressources) en fonction de la politique de gestion du réseau (RSVP, par exemple).
- **Services différenciés** : Les ressources du réseau sont réparties en fonction de la classification du trafic et de la priorité, ce qui donne un traitement préférentiel aux données avec des exigences de synchronisation strictes.

Le commutateur prend en charge DiffServ.

La fonction DiffServ contient un certain nombre de blocs de construction QoS conceptuels que vous pouvez utiliser pour construire un réseau de services différenciés. Utilisez ces mêmes blocs de différentes manières pour construire d'autres types d'architectures QoS.

Vous devez configurer trois blocs de construction QoS clés pour DiffServ :

- Classe
- Politique
- Service (affectation d'une stratégie à une interface directionnelle)

Classe

Vous pouvez classer les paquets entrants aux couches 2, 3 et 4 en examinant les informations suivantes pour un paquet :

- Adresse MAC source/destination
- EtherType
- Valeur de classe de service (priorité 802.1p) (première/seule balise VLAN)
- Plage d'ID VLAN (première/seule balise VLAN)
- Valeur de priorité 802.1p secondaire (balise VLAN seconde/interne)
- Plage d'ID VLAN secondaire (balise VLAN seconde/interne)
- Octet de type de service IP (également appelé : Bits TOS, valeur de priorité, valeur DSCP)

- Protocole de couche 4 (TCP, UDP, etc.)
- Ports source/destination de couche 4
- Adresse IP source/destination

Du point de vue de DiffServ, il existe deux types de classes :

- Classes de trafic DiffServ.
- Niveaux de service/classes de transfert DiffServ

Classes de trafic DiffServ.

Avec DiffServ, vous définissez les classes de trafic à suivre sur une interface d'entrée. Vous pouvez définir des classificateurs d'agrégat de comportement simple (BA) (DSCP) et une grande variété de classificateurs multi-champs (MF) :

- Couche 2 ; couches 3, 4 (IP uniquement)
- Basé sur le protocole
- Basé sur l'adresse

Vous pouvez combiner ces classificateurs avec des opérations logiques ET ou OU OU pour construire des classificateurs MF complexes (en spécifiant un type de classe *All* ou *any*, respectivement). C'est-à-dire qu'au sein d'une même classe, plusieurs critères de correspondance sont regroupés sous forme d'expression ET ou SÉQUENTIELLE OU, selon le type de classe défini. Seules les classes du même type peuvent être imbriquées ; l'imbrication de classes ne permet pas la négation (option *exclude*) de la classe référencée.

Pour configurer DiffServ, vous devez définir des niveaux de service, à savoir les classes de transfert/comportements par saut (PHB) identifiés par une valeur DSCP, sur l'interface de sortie. Vous définissez ces niveaux de service en configurant des classes BA pour chacun.

Créer une politique

Utilisez les stratégies DiffServ pour associer une collection de classes que vous configurez à une ou plusieurs instructions de stratégie QoS. Le résultat de cette association est appelé une politique.

Du point de vue de DiffServ, il existe deux types de politiques :

- **Politique de conditionnement du trafic** : Stratégie appliquée à une classe de trafic DiffServ
- **Stratégie de provisionnement des services** : Stratégie appliquée à un niveau de service DiffServ

Vous devez configurer manuellement les différentes instructions et règles utilisées dans les stratégies de conditionnement du trafic et de provisionnement des services pour obtenir respectivement les opérations TCS (Traffic Conditioning Specification) et SLS (Service Level Specification) souhaitées.

Politique de conditionnement du trafic

Le conditionnement du trafic concerne les actions effectuées sur le trafic entrant. Plusieurs actions QoS distinctes sont associées au conditionnement du trafic :

- **Abandonné** Déposez un paquet à l'arrivée. Ceci est utile pour émuler l'opération de liste de contrôle d'accès à l'aide de DiffServ, en particulier lorsque DiffServ et ACL ne peuvent pas coexister sur la même interface.
- **Marquage IP DSCP ou IP précedence** : Marquage/re-marquage du point de code DiffServ dans un paquet avec la valeur DSCP représentant le niveau de service associé à une classe de trafic DiffServ particulière. Alternativement, la valeur de priorité IP du paquet peut être marquée/re-marquée.
- **Marquage cos (802.1p)** : Définit le champ de priorité à trois bits dans le premier/seul en-tête 802.1p sur une valeur spécifiée lorsque des paquets sont transmis pour la classe de trafic. Un en-tête 802.1p est inséré si informatique n'existe pas déjà. Ceci est utile pour attribuer un niveau de priorité de couche 2 basé sur une définition de classe de transfert DiffServ (telle que la valeur de priorité DSCP ou IP) pour transmettre certaines caractéristiques QoS aux commutateurs en aval qui ne consultent pas systématiquement la valeur DSCP dans l'en-tête IP.
- **Maintien de l'ordre** : L'invention concerne un procédé permettant de limiter le trafic entrant associé à une classe particulière de sorte que le informatique soit conforme aux termes du TCS. Un traitement spécial peut être appliqué aux paquets hors profil qui dépassent la spécification de conformité ou sont non conformes.

La fonction DiffServ prend en charge les types de traitements (actions) de contrôle du trafic suivants :

- Envoyer Le paquet est transmis sans modification DiffServ.
- Abandonné Le paquet est abandonné.
- **Mark cos** : Les bits de priorité utilisateur 802.1p sont (re)marqués et transmis.
- **Mark DSCP** : Le paquet DSCP est (re)marqué et transmis.
- **Marquer la priorité IP** : La priorité IP du paquet est (re)marquée et transférée.
- **Connaissance du mode couleur** : Le maintien de l'ordre dans la fonction DiffServ utilise le mode *daltonien* ou le mode *couleur*. Le mode daltonien ignore la coloration (marquage) du paquet entrant. Le mode Color Aware prend en compte le marquage du paquet actuel lors de la détermination du résultat du contrôle. Une classe de trafic auxiliaire est utilisée conjointement avec la définition de police pour spécifier une valeur pour l'un des champs 802.1p, 802.1p secondaire, IP DSCP ou IP

Precedence désignant la valeur de couleur entrante à utiliser comme couleur conforme. En option, vous pouvez également spécifier la couleur de dépassement du trafic.

- **Affectation d'une file d'attente QoS** : Dirige un flux de trafic vers la file d'attente QoS spécifiée. Ceci permet à un classificateur de trafic de spécifier laquelle des files d'attente matérielles prises en charge est utilisée pour traiter les paquets appartenant à la classe.
- **Redirection...** Force un flux de trafic classifié vers un port de sortie spécifié (physique ou lag). Cela peut se produire en plus de toute action de marquage ou de maintien de l'ordre. informatique peut également être spécifié avec une affectation de file d'attente QoS.
- **Miroir de ports** Copie un flux de trafic classifié vers un port de sortie spécifié (physique ou lag). Cela peut se produire en plus de toute action de marquage ou de maintien de l'ordre. informatique peut également être spécifié avec une affectation de file d'attente QoS.
- **Total** Mise à jour des statistiques sur les octets et les paquets pour garder une trace de la gestion des données le long des chemins de trafic dans DiffServ. Dans cette fonctionnalité DiffServ, les compteurs ne sont pas explicitement configurés par l'utilisateur, mais sont conçus dans le système en fonction de la stratégie DiffServ créée. Pour plus d'informations, consultez la section [Statistiques des ports et des paquets EAP](#) à la page 1089.

Exemple de configuration DiffServ.

Pour créer une classe/stratégie DiffServ et attacher informatique à une interface de commutateur, procédez comme suit :

1. Sur la page Configuration de classe QoS, créez une nouvelle classe avec les paramètres suivants :

- **Nom de classe** : Class1
- **Type de classe** : Tout

Pour plus d'informations sur cette page, reportez-vous à [Configurer une classe DiffServ](#) à la page 785 la section .

2. Cliquez sur le lien hypertexte **Class1** pour afficher la page Configuration de classe DiffServ pour cette classe.
3. Configurez les paramètres suivants pour la classe 1 :
 - **Type de protocole** : UDP
 - Adresse IP source 192.12.1.0.

- Masque source 255.255.255.0.
- **Port source L4** : Autre, puis entrez 4567 comme valeur du port source.
- **Adresse IP de destination**. 192.12.2.0.
- **Masque de destination** : 255.255.255.0.
- **Port L4 de destination** : Autre, puis entrez 4568 comme valeur du port de destination.

Pour plus d'informations sur cette page, reportez-vous à [Configurer une classe DiffServ](#) à la page 785 la section .

4. Cliquez sur le bouton **Apply** (Appliquer).
5. Sur la page Configuration de la stratégie, créez une nouvelle stratégie avec les paramètres suivants :

- **Sélecteur de politique** : Policy1
- **Classe membre** : Class1

Pour plus d'informations sur cette page, reportez-vous à [Configurer une stratégie DiffServ](#) à la page 800 la section .

6. Cliquez sur le bouton **Add** (Ajouter).

La stratégie est ajoutée.

7. Cliquez sur le lien hypertexte **Policy1** pour afficher la page Configuration de la classe de règle de cette règle.
8. Configurez les attributs de stratégie comme suit :

- **Attribuer une file d'attente** : 3
- **Attribut de stratégie** : Politique simple
- **Mode couleur** : Couleur aveugle
- **Taux engagé** : 1000000 kbit/s
- **Taille de rafale validée** : 128 Ko
- **Confirmer l'action** : Envoyer
- **Action violer** : Abandonné

Pour plus d'informations sur cette page, reportez-vous à [Configurer une stratégie DiffServ](#) à la page 800 la section .

9. Sur la page Configuration du service, cochez la case en regard des interfaces 7 et 8 pour associer la stratégie à ces interfaces, puis cliquez sur le bouton **appliquer**. (Consultez la section .)

Tous les flux de paquets UDP destinés au réseau 192.12.2.0 avec une adresse IP source provenant du réseau 192.12.1.0 qui incluent un port source de couche 4 de 4567 et un

port de destination de 4568 à partir de ce commutateur sur les ports 7 et 8 sont affectés à la file d'attente matérielle 3.

Sur ce réseau, le trafic des applications de streaming utilise le port UDP 4567 comme source et 4568 comme destination. Ce trafic en temps réel étant sensible au temps, informatique est affecté à une file d'attente matérielle prioritaire. Par défaut, le trafic de données utilise la file d'attente matérielle 0, qui est désignée comme file d'attente de meilleur effort.

L'action confirmée sur ce flux consiste également à envoyer les paquets avec un débit engagé de 1000000 Kbps et une taille de rafale de 128 Ko. Les paquets qui ne respectent pas le débit validé et la taille des rafales sont abandonnés.

Contrôle d'accès au port 802.1X.

Les réseaux locaux (LAN) sont souvent déployés dans des environnements qui permettent aux périphériques non autorisés d'être physiquement connectés à l'infrastructure LAN ou aux utilisateurs non autorisés de tenter d'accéder au LAN via des équipements déjà connectés. Dans de tels environnements, vous pouvez restreindre l'accès aux services offerts par le réseau local aux utilisateurs et périphériques autorisés à utiliser ces services.

Le contrôle d'accès réseau basé sur les ports utilise les caractéristiques physiques des infrastructures LAN pour fournir un moyen d'authentification et d'autorisation des périphériques connectés à un port LAN avec des caractéristiques de connexion point à point. Si le processus d'authentification et d'autorisation échoue, le contrôle d'accès empêche l'accès à ce port. Dans ce contexte, un port est un point de connexion unique au LAN, tel qu'un port d'un pont MAC et une association entre des stations ou des points d'accès dans des LAN sans fil IEEE 802,11.1.

La norme IEEE 802,11 décrit un cadre architectural dans lequel l'authentification et les actions qui en découlent ont lieu. informatique définit également les exigences d'un protocole entre l'authentificateur (le système qui transmet une demande d'authentification au serveur d'authentification) et le demandeur (le système qui demande l'authentification), ainsi qu'entre l'authentificateur et le serveur d'authentification.

Le commutateur prend en charge un VLAN invité, ce qui permet aux utilisateurs non authentifiés d'accéder de manière limitée aux ressources réseau.

❗ Remarque: Vous pouvez utiliser les fonctionnalités QoS pour limiter le débit sur le VLAN invité afin de limiter les ressources réseau fournies par le VLAN invité.

Une autre fonctionnalité 802.1X est la possibilité de configurer un port pour activer ou désactiver la prise en charge du transfert de paquets EAPOL. Vous pouvez désactiver ou activer le transfert d'EAPOL lorsque 802.1X est désactivé sur le périphérique.

Les ports d'un commutateur d'authentification 802.1X permettent à informatique d'offrir des services à d'autres systèmes accessibles via le réseau local. Le contrôle d'accès au réseau basé sur les ports permet de contrôler le fonctionnement des ports d'un commutateur afin de s'assurer que l'accès à ses services n'est autorisé que par les systèmes autorisés à le faire.

Le contrôle d'accès aux ports permet de prévenir l'accès non autorisé des demandeurs aux services offerts par un système. Le contrôle de l'accès à un commutateur et au réseau local auquel informatique est connecté peut être souhaitable si vous restreignez l'accès aux ports de pont accessibles au public ou aux réseaux locaux ministériels.

Le contrôle d'accès est réalisé par l'application de l'authentification des demandeurs qui sont rattachés aux ports contrôlés d'un authenticateur. Le résultat du processus d'authentification détermine si le demandeur est autorisé à accéder aux services sur ce port contrôlé.

Une entité d'accès au port (PAE) peut adopter l'un des deux rôles distincts au sein d'une interaction de contrôle d'accès :

1. **Authentification.** Port qui applique l'authentification avant d'autoriser l'accès aux services disponibles via ce port.
2. **Demandeur** : Port qui tente d'accéder aux services offerts par l'authentificateur.

En outre, un serveur d'authentification est requis. Il s'agit d'un périphérique qui exécute la fonction d'authentification nécessaire pour vérifier les informations d'identification du demandeur au nom de l'authentificateur. Pour effectuer un échange d'authentification, un authenticateur, un demandeur et un serveur d'authentification sont requis.

Le commutateur prend uniquement en charge le rôle d'authentificateur, dans lequel la consultation est responsable de la communication avec le demandeur.

L'authentificateur PAE est également chargé de soumettre les informations reçues du demandeur au serveur d'authentification pour les justificatifs à vérifier, qui détermine l'état d'autorisation du port. L'authentificateur PAE contrôle l'état autorisé/non autorisé du port contrôlé en fonction du résultat du processus d'authentification basé sur RADIUS.

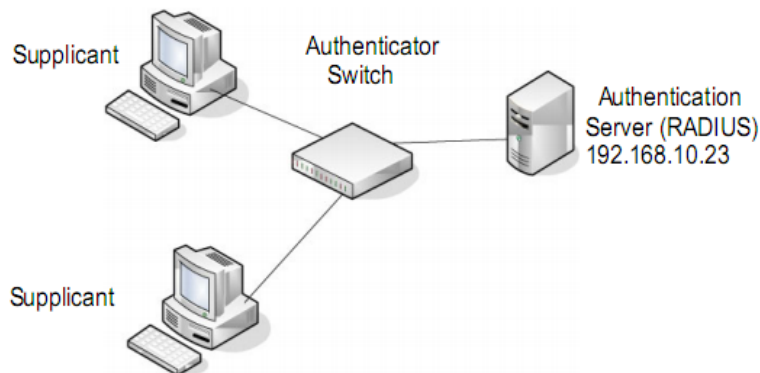


Illustration 1 : Rôles d'authentification 802.1X.

802.1X exemple de configuration .

Cet exemple montre comment configurer le commutateur de sorte que l'authentification basée sur 802.1X soit requise sur les ports d'une salle de conférence d'entreprise (5 à 8). Ces ports sont disponibles pour les visiteurs et doivent être authentifiés avant que l'accès au réseau ne soit accordé. L'authentification est gérée par un serveur RADIUS externe. Lorsque le visiteur est authentifié avec succès, le trafic est automatiquement affecté au VLAN invité. Cet exemple suppose qu'un VLAN a été configuré avec l'ID VLAN 150 et le nom VLAN invité.

1. Sur la page authentification du port , sélectionnez les ports **5, 6, 7 et 8**.
2. Dans le menu **contrôle des ports**, sélectionnez **non autorisé**.

La sélection dans le menu **Port Control** pour tous les autres ports sur lesquels l'authentification n'est pas nécessaire doit être **autorisée**. Lorsque la sélection dans le menu **contrôle de port** est **autorisé**, le port est placé inconditionnellement dans un état d'autorisation forcée et ne nécessite aucune authentification. Lorsque la sélection dans le menu **contrôle de port** est **Auto**, l'authentificateur consultation définit le mode de port contrôlé.

3. Dans le champ **VLAN invité** pour les ports 5 à 8, entrez **150** pour attribuer ces ports au VLAN invité.

Vous pouvez configurer des paramètres supplémentaires pour contrôler l'accès au réseau via les ports. Pour plus d'informations sur les paramètres, reportez-vous à la section [Configurer une interface de sécurité de port](#) à la page 920.

4. Cliquez sur le bouton **Apply** (Appliquer).
5. Sur la page de configuration 802.1X, définissez l'état d'authentification basée sur le port et le mode VLAN invité sur **Activer**, puis cliquez sur le bouton **appliquer** (voir [Configurez le mode de sécurité du port global](#) à la page 919).

Cet exemple utilise les valeurs par défaut pour les paramètres d'authentification du port, mais vous pouvez configurer plusieurs paramètres supplémentaires. Par exemple, le champ **EAPOL Flood mode** vous permet d'activer le transfert des trames EAPOL lorsque 802.1X est désactivé sur le périphérique.

6. Sur la page Configuration du serveur RADIUS, configurez un serveur RADIUS avec les paramètres suivants :
 - **Server Address** (Adresse du serveur). 192.168.10.23
 - **Secret configuré** : Oui
 - **Secret** : secret123
 - **Actif**. Principal

Pour plus d'informations, consultez [serveurs RADIUS](#) à la page 831.

7. Cliquez sur le bouton **Add** (Ajouter).
8. Sur la page Authentication List (liste d'authentification), configurez la liste par défaut pour utiliser RADIUS comme première méthode d'authentification (voir [Configurez une liste d'authentification de connexion](#) à la page 850).

Cet exemple active la sécurité de port basée sur 802.1X sur le commutateur et invite les hôtes connectés sur les ports 5 à 8 à effectuer une authentification basée sur 802.1X. Le commutateur transmet les informations d'authentification au serveur RADIUS configuré.

Protocole Spanning Tree multiple .

Le protocole STP (Spanning Tree Protocol) s'exécute sur des réseaux pontés pour aider à éliminer les boucles. Si une boucle de pont se produit, le réseau peut être inondé de trafic. IEEE 802.1s multiple Spanning Tree Protocol (MSTP) prend en charge plusieurs instances de Spanning Tree pour canaliser efficacement le trafic VLAN sur différentes interfaces. Chaque instance du Spanning Tree se comporte de la manière spécifiée dans IEEE 802.1w, Rapid Spanning Tree, avec de légères modifications dans le fonctionnement mais pas dans l'effet final (le principal des effets est la transition rapide du port à l'état de transfert).

La différence entre RSTP et STP traditionnel (IEEE 802.1D) réside dans la capacité de configurer et de reconnaître la connectivité duplex intégral et les ports connectés aux stations d'extrémité, ce qui permet une transition rapide du port à l'état de transfert et la suppression de la notification de modification de topologie. Ces fonctions sont représentées par les paramètres pointtopoint et edgeport. MSTP est compatible avec RSTP et STP. informatique se comporte d'une manière appropriée pour les ponts STP et RSTP.

Un pont MSTP peut être configuré pour se comporter entièrement comme un pont RSTP ou un pont STP. Ainsi, un pont IEEE 802.1s prend également en charge IEEE 802.1w et IEEE 802.1D.

L'algorithme et le protocole MSTP fournissent une connectivité simple et complète pour les trames attribuées à n'importe quel VLAN via un réseau local ponté comprenant des périphériques réseau interconnectés arbitrairement, chacun fonctionnant avec MSTP, STP ou RSTP. MSTP permet aux trames attribuées à différents VLAN de suivre des chemins distincts, chacun basé sur une instance MSTI (multiple Spanning Tree instance) indépendante, dans plusieurs régions MST (Spanning Tree) composées de LAN et/ou de ponts MSTP. Ces régions et les autres ponts et réseaux locaux sont connectés en un seul CST (Common Spanning Tree). (PROJET IEEE P802.1S/D13)

MSTP connecte tous les ponts et LAN avec un seul CIST (Common and Internal Spanning Tree). Le CIST prend en charge la détermination automatique de chaque région MST, en choisissant son étendue maximale possible. La connectivité calculée pour le CIST fournit le CST pour l'interconnexion de ces régions, et un Spanning Tree interne (IST) dans chaque région.

MSTP garantit que les trames avec un ID VLAN sont attribuées à un seul des MSTI ou IST dans la région, que l'attribution est cohérente entre tous les périphériques réseau de la région et que la connectivité stable de chaque MSTI et IST à la limite de la région correspond à celle du CST.

MSTP assure ce qui suit :

- Les trames avec un ID VLAN sont attribuées à un seul MSTI ou IST dans la région
- l'affectation est cohérente entre tous les périphériques réseau de la région
- La connectivité stable de chaque MSTI et IST à la limite de la région correspond à celle du CST

La topologie active stable du réseau local ponté par rapport aux trames classifiées de manière cohérente comme appartenant à n'importe quel VLAN réseau local et périphérique connecte donc simplement et entièrement tous les réseaux locaux et périphériques réseau à travers le réseau, bien que les trames appartenant à différents réseaux locaux virtuels puissent prendre des chemins différents dans n'importe quelle région, selon LE PROJET IEEE P802.1s/D13.

Tous les ponts, qu'ils utilisent STP, RSTP ou MSTP, envoient des informations dans des messages de configuration via des unités de données de protocole de pont (BPDU) pour attribuer des rôles de port qui déterminent la participation de chaque port à une

topologie active entièrement et simplement connectée basée sur un ou plusieurs Spanning Tree. L'information communiquée est connue sous le nom de vecteur de priorité de l'arbre maximal. La structure BPDU de chacun de ces protocoles est différente. Un pont MSTP transmet la BPDU appropriée en fonction du type de BPDU reçu à partir d'un port particulier.

Une région MST comprend un ou plusieurs ponts MSTP avec le même identificateur de configuration MST, utilisant les mêmes MSTI, et sans ponts rattachés qui ne peuvent pas recevoir et transmettre des BPDU MSTP. L'identificateur de configuration MST comprend les composants suivants :

- Sélecteur de format d'identificateur de configuration
- Nom de la configuration
- Niveau de révision de la configuration
- Résumé de configuration : Signature 16 octets de type HMAC-MD5 créée à partir de la table de configuration MST (mappage ID VLAN vers MSTID)

Etant donné qu'il existe plusieurs instances de Spanning Tree, un état MSTP est maintenu par port, par instance (ou par port, par VLAN, car n'importe quel VLAN peut être dans un seul MSTI ou CIST). Par exemple, le port A peut transférer pour l'instance 1 tout en rejetant pour l'instance 2. Les états des ports ont changé depuis la spécification IEEE 802.1D.

Pour prendre en charge plusieurs Spanning Tree, configurez un pont MSTP avec une affectation univoque d'ID VLAN (VID) aux Spanning Tree. Pour une telle configuration, vérifiez les points suivants :

- L'attribution des VID aux FID est sans ambiguïté.
- Chaque FID pris en charge par le pont est alloué à exactement une instance Spanning Tree.

La combinaison de l'allocation VID à FID, puis FID à MSTI définit un mappage des VID aux instances Spanning Tree, représentées par la table de configuration MST.

Grâce à cette allocation, nous nous assurons que chaque VLAN est assigné à un et un seul MSTI. Le CIST est également une instance de Spanning Tree avec un MSTID de 0.

Les VID peuvent ne pas être alloués à une instance, mais chaque VLAN doit être alloué à l'une des autres instances de Spanning Tree.

La partie de la topologie active du réseau qui connecte deux ponts quelconques dans la même région MST traverse uniquement les ponts MST et les LAN dans cette région, et jamais les ponts de quelque nature que ce soit en dehors de la région. En d'autres termes, la connectivité au sein de la région est indépendante de la connectivité externe.

Exemple de configuration MSTP.

Cet exemple montre comment créer une instance MSTP à partir du commutateur. L'exemple de réseau comprend trois commutateurs différents qui desservent différents emplacements du réseau. Dans la figure suivante, les ports 1/0/1-1/0/5 sont connectés à des stations hôtes, de sorte que ces liaisons ne sont pas soumises à des boucles réseau. Les ports 1/0/6-1/0/8 sont connectés aux commutateurs 1, 2 et 3.

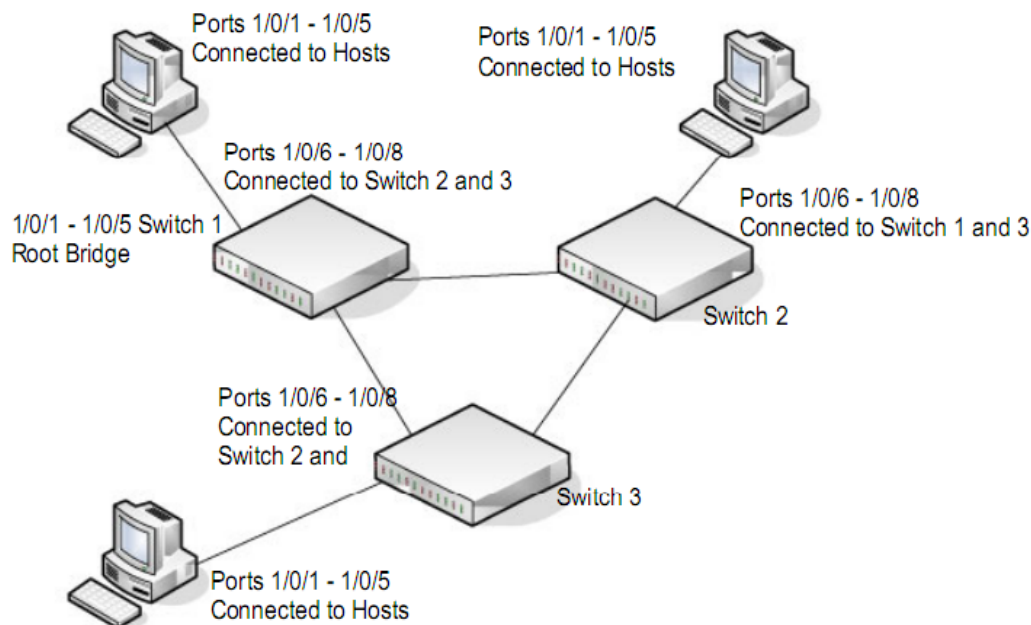


Illustration 2 : Exemple de configuration MSTP

Effectuez les procédures suivantes sur chaque commutateur pour configurer MSTP :

1. Utilisez la page de configuration VLAN pour créer les VLAN 300 et 500 (voir [Modifiez les paramètres d'allocation VLAN internes](#) à la page 315).
2. Sur la page VLAN Membership, incluez les ports 1 à 8 en tant que membres balisés (T) ou non balisés (U) de VLAN 300 et VLAN 500 (voir [Modifiez les paramètres d'allocation VLAN internes](#) à la page 315).
3. Sur la page STP Configuration (Configuration STP), activez l'option Spanning Tree State (État Spanning Tree) [Configurez les paramètres de l'interface CST](#) à la page 384) (voir).

Utilisez les valeurs par défaut pour le reste des paramètres de configuration STP. Par défaut, le mode de fonctionnement STP est MSTP et le nom de configuration est l'adresse MAC du commutateur.

4. Sur la page CST Configuration, définissez la valeur de priorité du pont pour chacun des trois commutateurs afin de forcer le commutateur 1 à être le pont racine :

- **Interrupteur 1** : 4096
- **Interrupteur 2** : 12288
- **Interrupteur 3** : 20480

❗ **Remarque:** Les valeurs de priorité du pont sont des multiples de 4096.

Si vous ne spécifiez pas de pont racine et que tous les commutateurs se voient attribuer la même valeur de priorité de pont, le commutateur dont l'adresse MAC est la plus basse est choisi comme pont racine (voir [Configurez les paramètres CST et affichez l'état CST](#) à la page 381).

5. Sur la page CST Port Configuration (Configuration du port CST), sélectionnez les ports 1 à 8 et sélectionnez **Enable (Activer)** dans le menu **STP Status (État STP)** (voir [Configurez les paramètres de l'interface CST](#) à la page 384).
6. Cliquez sur le bouton **Apply** (Appliquer).
7. Sélectionnez les ports 1 à 5 (ports périphériques), puis sélectionnez **Activer** dans le menu **Fast Link**.

Comme les ports de périphérie ne sont pas exposés aux boucles réseau, les ports sur lesquels Fast Link est activé passent directement à l'état de transfert.

8. Cliquez sur le bouton **Apply** (Appliquer).
Vous pouvez utiliser la page Etat du port CST pour afficher les informations relatives à l'arborescence de recouvrement de chaque port.
9. Sur la page Configuration MST ([Gérer les instances MST](#) à la page 390), créez une instance MST avec les paramètres suivants :

- **ID MST** : 1
- **Priority** (Priorité). Utiliser la valeur par défaut (32768)
- Identifiant VLAN : 300

10. Cliquez sur le bouton **Add** (Ajouter).
11. Créez une deuxième instance MST avec les paramètres suivants :

- **ID MST** : 2
- **Priority** (Priorité). 49152
- Identifiant VLAN : 500

12. Cliquez sur le bouton **Add** (Ajouter).

Dans cet exemple, supposons que le commutateur 1 est devenu le pont racine de l'instance MST 1 et que le commutateur 2 est devenu le pont racine de l'instance MST 2. Le commutateur 3 prend en charge les hôtes du service commercial (ports 1, 2 et 3) et du service RH (ports 4 et 5). Les commutateurs 1 et 2 incluent également des hôtes dans les départements des ventes et des RH. Les hôtes connectés à partir du

commutateur 2 utilisent VLAN 500, MST instance 2 pour communiquer directement avec les hôtes du commutateur 3. De même, les hôtes du commutateur 1 utilisent VLAN 300, instance 1 de MST pour communiquer directement avec les hôtes du commutateur 3.

Les hôtes utilisent différentes instances de MSTP pour utiliser efficacement les liaisons à travers le commutateur. Le même concept peut être étendu à d'autres commutateurs et à plus d'instances de MSTP.

Interfaces de routage VLAN

Les VLAN divisent les domaines de broadcast dans un environnement LAN. Lorsque des hôtes d'un VLAN doivent communiquer avec des hôtes d'un autre VLAN, le trafic doit être acheminé entre eux. C'est ce qu'on appelle le routage inter-VLAN. Sur le commutateur, l'information est réalisée en créant des interfaces de couche 3 (interfaces virtuelles de commutateur [SVI]).

Lorsqu'un port est activé pour le pontage (valeur par défaut) plutôt que pour le routage, tout le traitement de pont normal est effectué pour un paquet entrant, qui est ensuite associé à un VLAN. Son adresse MAC de destination et son ID VLAN sont utilisés pour effectuer des recherches dans la table d'adresses MAC. Si le routage est activé pour le VLAN et que l'adresse MAC de destination d'un paquet de monodiffusion entrant est celle de l'interface pont-routeur interne, le paquet est routé. Un paquet de multidiffusion entrant est transmis à tous les ports du VLAN, ainsi qu'à l'interface pont-routeur interne, si l'information a été reçue sur un VLAN routé.

Comme un port peut être configuré pour appartenir à plusieurs VLAN, le routage VLAN peut être activé pour tous les VLAN du port, ou pour un sous-ensemble. Le routage VLAN peut être utilisé pour permettre à plusieurs ports physiques de résider sur le même sous-réseau. L'information peut également être utilisée lorsqu'un VLAN s'étend sur plusieurs réseaux physiques, ou lorsqu'une segmentation ou une sécurité supplémentaire est requise. Un port peut être un port VLAN ou un port de routeur, mais pas les deux. Cependant, un port VLAN peut faire partie d'un VLAN qui est lui-même un port de routeur.

Procédez comme suit pour configurer un commutateur afin d'effectuer un routage interVLAN pour IPv4 :

1. Utilisez la page Configuration IP pour activer le routage IPv4 sur le commutateur.
Par défaut, le routage IPv4 est activé. Pour plus d'informations sur cette étape, reportez-vous à la section [Gérer les paramètres de routage IPv4 globaux](#) à la page 532.
2. Déterminez les adresses IP que vous souhaitez attribuer à l'interface VLAN sur le commutateur.

Pour que le commutateur puisse acheminer entre les VLAN, les interfaces VLAN doivent être configurées avec une adresse IP. Lorsque le commutateur reçoit un paquet destiné à un autre sous-réseau ou VLAN, il examine la table de routage pour déterminer où transférer le paquet. Le paquet est ensuite transmis à l'interface VLAN de la destination. L'information est ensuite envoyée au port auquel le périphérique final est connecté.

3. Utilisez la page Assistant routage statique VLAN pour créer un VLAN de routage, configurer l'adresse IP et le masque de sous-réseau, puis ajouter les ports membres. Pour plus d'informations sur cette étape, reportez-vous à la section Créez un VLAN de routage à l'aide de l'assistant de routage statique VLAN à la page 566.

A

Paramètres logiciels par défaut et spécifications matérielles

L'annexe contient les sections suivantes :

- [Accéder aux paramètres par défaut de l' interface utilisateur principale du commutateur](#)
- [Paramètres par défaut des fonctions système](#)
- [Commutation des paramètres par défaut des fonctions](#)
- [Paramètres par défaut des fonctions de routage, OSPF, OSPFv3 et multicast](#)
- [QoS propose les paramètres par défaut](#)
- [Paramètres par défaut des fonctions de sécurité](#)
- [Paramètres par défaut des fonctions de surveillance](#)
- [Spécifications techniques générales du matériel](#)
- [Spécifications techniques matérielles spécifiques au modèle](#)

❗ **Remarque:** Pour plus d'informations sur les caractéristiques et les fonctionnalités du commutateur, y compris les paramètres maximum pour de nombreuses fonctionnalités, consultez la fiche technique, que vous pouvez télécharger sur le site netgear.com/support/download/.

Accéder aux paramètres par défaut de l'interface utilisateur principale du commutateur

Le tableau suivant décrit les paramètres par défaut pour l'accès à l'interface utilisateur principale du commutateur.

(Les paramètres en lecture seule ne sont pas inclus dans le tableau mais peuvent être inclus dans la fiche technique, que vous pouvez télécharger en visitant netgear.com/support/download/.)

Table 196 : Paramètres par défaut pour l'accès à l'interface utilisateur principale du commutateur

Fonction	Par défaut
Adresse IP pour VLAN de gestion	169 254 100 100
Adresse IP du port de service	192.168.0.239
Masque de sous-réseau	255.255.0.0
Passerelle par défaut	0.0.0.0
ID du VLAN de gestion	1
Protocole de port de service	Client DHCP activé
Utilisateur Admin	Nom d'utilisateur : admin (accès en lecture/écriture) Nouveau mot de passe : Aucun mot de passe (c'est-à-dire que le mot de passe est vide), mais lors de la première connexion, l'utilisateur admin doit spécifier un mot de passe. Type de chiffrement SHA512 Mode d'authentification multifacteur : Désactivé(e)
Guest user (Utilisateur invité).	Nom d'utilisateur : invité (accès en lecture seule) Nouveau mot de passe : Aucun mot de passe (c'est-à-dire que le mot de passe est vide), mais lors de la première connexion, l'utilisateur invité doit spécifier un mot de passe. Type de chiffrement SHA512 Mode d'authentification multifacteur : Désactivé(e)
Longueur minimale des mots de passe admin et guest	Huit caractères
Mode de gestion IPv6	Sous tension
Configuration automatique de l'adresse IPv6	Désactivé(e)

Paramètres par défaut des fonctions système

Le tableau suivant décrit les paramètres par défaut des fonctionnalités système que vous pouvez configurer.

(Les paramètres en lecture seule ne sont pas inclus dans le tableau mais peuvent être inclus dans la fiche technique, que vous pouvez télécharger en visitant netgear.com/support/download/.)

Table 197 : Paramètres par défaut des fonctions système

Nom/paramètre de la fonction	Par défaut
Temps, Global	
Source d'horloge	NTP
Heure, NTP, Global	
Mode d'authentification NTP	Sous tension
Mode client de diffusion NTP	Désactivé(e)
Délai de diffusion	3000
Interface source	VLAN 1
Heures de décalage	0
Minutes de décalage	0
Heure, serveur NTP	
Type de serveur	DNS (pour chaque serveur par défaut)
Adresse	time-a.netgear.com time-c.netgear.com
Version	4 (pour chaque serveur par défaut)
ID de clé	0 (pour chaque serveur par défaut)
Intervalle d'interrogation minimum	6 (pour chaque serveur par défaut)
Intervalle d'interrogation maximum	10 (pour chaque serveur par défaut)
Préférences	Aucun
Rafale	Oui
IBurst	Oui
Heure, heure d'été	

Table 197 : Paramètres par défaut des fonctions système (A continué)

Nom/paramètre de la fonction	Par défaut
Heure d'été	Désactivé(e)
DNS	
État DNS	Sous tension
Numéro de nouvelle tentative	2
Délai de réponse dépassé	3
Interface source	VLAN 1
serveur DNS	8.8.8.8
Préférence de modèle SDM	
Préférence de modèle SDM	IPv4-Basic
Ethernet vert, Global	
Mode de mise hors tension automatique	Désactivé(e)
Mode EEE	Désactivé(e)
Ethernet vert, interface	
Mode de mise hors tension automatique	Désactivé(e)
Mode EEE	Désactivé(e)
Mode administrateur de détection d'énergie	Désactivé(e)
EEE mode admin	Désactivé(e)
Temps d'inactivité de transmission EEE	600
EEE transmettre l'heure de réveil	17
Historique LPI Ethernet vert	
Intervalle d'échantillonnage	3600
Nombre maximum d'échantillons à conserver	168
Bonjour	
Mode Admin	Sous tension
Precision Time Protocol, Global	
Mode Admin	Désactivé(e)
Precision Time Protocol, interface	
Mode configuré	Désactivé(e)
Serveur TFTP	

Table 197 : Paramètres par défaut des fonctions système (A continué)

Nom/paramètre de la fonction	Par défaut
Mode Admin	Désactivé(e)
Serveur DHCP	
Aucun serveur DHCP configuré	
Mode Admin	Désactivé(e)
Nombre de paquets ping	2
Mode de consignation des conflits	Sous tension
Mode automatique BOOTP	Désactivé(e)
Relais DHCP	
Aucun relais DHCP configuré	
Nombre maximal de sauts	4
Mode Admin	Désactivé(e)
Temps d'attente minimum	0
Mode option ID circuit	None (Aucun)
Mode de remplacement du serveur	Désactivé(e)
Relais DHCP L2, global	
Aucun relais DHCP L2 configuré	
Mode Admin	Désactivé(e)
Relais DHCP L2, interface	
Mode Admin	Désactivé(e)
82 mode de confiance des options	Désactivé(e)
Mode sans option82	Abandonné
Relais UDP	
Aucun relais UDP configuré	
Mode Admin	Désactivé(e)
Serveur DHCPv6, global	
Aucun serveur DHCPv6 configuré	
Mode Admin	Désactivé(e)
Serveur DHCPv6, interface	
Mode Admin	Désactivé(e)

Table 197 : Paramètres par défaut des fonctions système (A continué)

Nom/paramètre de la fonction	Par défaut
Relais DHCPv6	
Aucun relais DHCPv6 configuré	
Mode Admin	Désactivé(e)
Configuration PoE (modèles PoE+ et PoE++ uniquement)	
Seuil d'utilisation du système	90 pour cent
Mode de gestion de l'alimentation	Dynamique
Pièges	Sous tension
Configuration du port PoE (modèles PoE+ et PoE++ uniquement)	
Puissance du port	Sous tension
Priorité des ports	Faibles
Mode de puissance	802.3at pour les modèles PoE+ 802 bt pour les modèles PoE++
Type de limite de puissance	Classe
Limite de puissance (W)	90.90
Type de détection	4ptdot3af
Programmation de la minuterie	None (Aucun)
SNMPv1/v2	
Configuration de la communauté	None (Aucun)
Configuration de trappe	None (Aucun)
Drapeaux d'interruption SNMPv1/v2	
Authentification	Sous tension
Liaison haut/bas	Sous tension
Utilisateurs multiples	Sous tension
Spanning Tree	Sous tension
Listes de contrôle d'accès (ACL)	Désactivé(e)
Portail captif	Désactivé(e)
DVMRP	Désactivé(e)
PIM	Désactivé(e)
PoE (pour les modèles PoE+ et PoE++ uniquement)	Sous tension

Table 197 : Paramètres par défaut des fonctions système (A continué)

Nom/paramètre de la fonction	Par défaut
Interruptions OSPFv2, erreurs	Tous désactivés
Pièges OSPFv2, LSA	Tous désactivés
Interruptions OSPFv2, débordement	Tous désactivés
Interruptions OSPFv2, retransmettre	Tous désactivés
Interruptions OSPFv2, changement d'état	Tous désactivés
Interruptions OSPFv3, erreurs	Tous désactivés
Pièges OSPFv3, LSA	Tous désactivés
Interruptions OSPFv3, débordement	Tous désactivés
Interruptions OSPFv3, retransmettre	Tous désactivés
Interruptions OSPFv3, changement d'état	Tous désactivés
État du module d'alimentation	Sous tension
Etat du ventilateur	Sous tension
Etat de la température	Sous tension
VRRP	Sous tension
Notification MAC	Désactivé(e)
SNMPv3	
Nom d'utilisateur	admin
Mode d'accès SNMPv3	Lecture/écriture
Protocole d'authentification	SHA512
Protocole de chiffrement	None (Aucun)
Configuration de trappe	None (Aucun)
LLDP, Global	
Intervalle annoncé TLV	30
Multiplieur de maintien	4
Délai de réinitialisation	2
Délai de transmission	5
LLDP, interface	
Transmission	Sous tension
Réception	Sous tension

Table 197 : Paramètres par défaut des fonctions système (A continué)

Nom/paramètre de la fonction	Par défaut
Notifier	Sous tension
TLV en option (description du port, nom du système, description du système, capacités du système)	Tous activés
Information du responsable	Sous tension
LLDP-MED, Global	
Comptage de répétitions de démarrage rapide	3
LLDP-MED, interface	
Statut MÉD	Sous tension
État de notification	Sous tension
Valeurs de longueur de type de transmission (capacités MED, stratégie réseau, identification de l'emplacement, MDI-PSE étendu, informations d'inventaire)	Tous activés
Dépendance de liens	
Aucun configuré	
ISDP, Global	
Mode Admin	Sous tension
Minuterie	30
Durée de maintien	180
Publicités de la version 2	Sous tension
ISDP, interface	
Mode Admin	Sous tension
Programmations de minuterie	
Aucun programme de minuterie configuré	

Commutation des paramètres par défaut des fonctions

Le tableau suivant décrit les paramètres par défaut des fonctions de commutation que vous pouvez configurer.

(Les paramètres en lecture seule ne sont pas inclus dans le tableau mais peuvent être inclus dans la fiche technique, que vous pouvez télécharger en visitant netgear.com/support/download/.)

Table 198 : Commutation des paramètres par défaut des fonctions

Nom/paramètre de la fonction	Par défaut
VLAN, Global	
Base d'allocation VLAN interne	4093
Politique interne d'allocation de VLAN	Croissant
VLAN par défaut (ID)	1 (tous les ports sont membres)
Nom VLAN par défaut	Par défaut
VLAN Trunking, Global	
Mode Admin	Sous tension
Ports de commutation, interface	
Mode de port de commutation	Partagé
Accéder à l'ID VLAN	1
ID VLAN natif	1
VLAN autorisés par agrégation	1-4093
PVID de port, interface	
PVID	1
Membre VLAN	1
Etiquette VLAN :	None (Aucun)
Cadre acceptable	Admettez tout
Filtrage d'entrée	Désactivé(e)
Priorité des ports	0
DVLAN, interface	
Mode Admin	Désactivé(e)
Voice VLAN, monde	
Mode Admin	Désactivé(e)
Voice VLAN, interface	
Mode interface	Désactivé(e)
Valeur	0
Mode de neutralisation cos	Désactivé(e)

Table 198 : Commutation des paramètres par défaut des fonctions (A continué)

Nom/paramètre de la fonction	Par défaut
Mode d'authentification	Sous tension
Valeur DSCP	0
GARP, Global	
Mode GVRP	Désactivé(e)
Mode GMRP	Désactivé(e)
GARP, interface	
Mode GVRP	Désactivé(e)
Mode GMRP	Désactivé(e)
Rejoindre le minuteur	20
Quitter le minuteur	60
Laisser tous les minuteurs	1000
Basé sur le protocole Auto-VoIP, Global	
Type de hiérarchisation	Classe de trafic
Valeur de classe	6
Interface basée sur le protocole Auto-VoIP	
Mode VoIP automatique	Désactivé(e)
Auto-VoIP basé sur oui, Global	
ID VLAN VoIP automatique	Aucun (0)
Priorité basée sur oui	7
Table OUI	00 :01 :E3 SIEMENS 00:03:6B CISCO1 00:12:43 CISCO2 00:0F:E2 H3C 00 :60 :B9 NITSUKO 00 :D0 :1E PINTEL 00 :E0 :75 VERILINK 00 :E0 :BB 3COM 00:04:0D AVAYA1 00:1B:4F AVAYA2 00 :04 :13 SNOM
Interface auto-VoIP basée sur oui	

Table 198 : Commutation des paramètres par défaut des fonctions (A continué)

Nom/paramètre de la fonction	Par défaut
Mode VoIP automatique	Désactivé(e)
iSCSI	
État iSCSI	Désactivé(e)
Profil QoS	Balise de priorité VLAN
Balise de priorité VLAN	5
DSCP	46
Remarque	Sous tension
Durée de vieillissement iSCSI	10
Cibles iSCSI, ports TCP	860 3260
STP, Global	
Mode d'administration Spanning Tree	Sous tension
Forcer la version du protocole	EEE 802.1w
Nom de la configuration	adresse MAC
Niveau de révision de la configuration	0
Transfert des BPDU lorsque le protocole STP est désactivé	Désactivé(e)
Protection BPDU	Désactivé(e)
Filtre BPDU	Désactivé(e)
Dorsale rapide	Désactivé(e)
Liaison montante rapide	Désactivé(e)
Fréquence de mise à jour max	150
CST, Global	
Priorité du pont	32768
Âge maximum du pont	20
Retard d'avance du pont	15
Sauts maximaux du Spanning Tree	20
Nombre de maintenances Tx du Spanning Tree	6
CST, interface	

Table 198 : Commutation des paramètres par défaut des fonctions (A continué)

Nom/paramètre de la fonction	Par défaut
Priorité des ports	128
Port périphérique Admin	Désactivé(e)
Coût du chemin du port	0
Coût de chemin de port calculé automatiquement	Sous tension
Coût du chemin du port externe	0
Coût de chemin de port externe calculé automatiquement	Sous tension
Filtre BPDU	Désactivé(e)
Transfert BPDU	Désactivé(e)
Arête automatique	Sous tension
Protège-racines	Désactivé(e)
Protection contre les boucles	Désactivé(e)
Protection TCN	Désactivé(e)
Mode port	Sous tension
MST, Global	
ID MST	0
Priorité	32768
Identifiant VLAN	1
PVST, VLAN	
Identifiant VLAN	1
Source	None (Aucun)
Bonjour Time	2
Temps avant	15
Âge maximum	20
Priorité	32768
PVST, interface	
Priorité	128
Coût	0
Coût calculé automatiquement	Sous tension

Table 198 : Commutation des paramètres par défaut des fonctions (A continué)

Nom/paramètre de la fonction	Par défaut
igmp snooping, monde	
Mode Admin	Sous tension
Validez l'en-tête IP IGMP	Sous tension
Mode Querier proxy	Sous tension
Signaler le mode inondation	Sous tension
Exclure le mode interface Mrouter	Sous tension
Quittez rapidement le mode d'affectation automatique	Sous tension
Mode IGMP plus	Sous tension
igmp snooping, interface	
Mode Admin	Désactivé(e)
Intervalle d'adhésion	600
Temps de réponse maximum	120
Heure d'expiration	300
Départ rapide	Désactivé(e)
Interrogateur proxy	Sous tension
igmp snooping, VLAN	
Identifiant VLAN	1
Mode Admin	Sous tension
Départ rapide	Sous tension
Intervalle d'adhésion	600
Temps de réponse maximum	120
Délai d'expiration du routeur multicast	300
Suppression de rapport	Désactivé(e)
Interrogateur proxy	Sous tension
Signaler le mode inondation	Sous tension
Exclure le mode interface Mrouter	Sous tension
Mode IGMP plus	Sous tension
igmp snooping, routeur multidiffusion, interface	
Routeur multidiffusion	Désactivé(e)

Table 198 : Commutation des paramètres par défaut des fonctions (A continué)

Nom/paramètre de la fonction	Par défaut
igmp snooping, Querier, Global	
Mode administrateur Querier	Sous tension
Adresse de l'interrogateur de surveillance	None (Aucun)
Version , ()	2
Intervalle de requête	60
Intervalle d'expiration du Querier	180
igmp snooping, Querier, VLAN	
Identifiant VLAN	1
Querier Election participe mode	Sous tension
Adresse du Querier VLAN :	None (Aucun)
MLD Snooping, Global	
Mode administrateur MLD Snooping	Sous tension
Mode Querier proxy	Sous tension
Signaler le mode inondation	Sous tension
Exclure le mode interface Mrouter	Sous tension
Mode MLD plus	Sous tension
MLD Snooping, interface	
Mode Admin	Désactivé(e)
Intervalle d'adhésion	260
Temps de réponse maximum	10
Heure d'expiration	300
Départ rapide	Désactivé(e)
Interrogateur proxy	Sous tension
MLD Snooping, VLAN	
Identifiant VLAN	1
Départ rapide	Sous tension
Intervalle d'adhésion	260
Temps de réponse maximum	10
Délai d'expiration du routeur multicast	300

Table 198 : Commutation des paramètres par défaut des fonctions (A continué)

Nom/paramètre de la fonction	Par défaut
Mode Querier proxy	Sous tension
Exclure le mode interface Mrouter	Sous tension
Mode MLD plus	Sous tension
MLD Snooping, routeur Multicast, interface	
Routeur multidiffusion	Désactivé(e)
MLD Snooping, Querier, Global	
Mode administrateur Querier	Désactivé(e)
Adresse Querier	None (Aucun)
Intervalle de requête	60
Intervalle d'expiration du Querier	60
Dossier du conducteur, mondial	
Conducteur en cours d'exécution	Désactivé(e)
VLAN multicast du dossier conducteur	1
Temps de réponse à la requête globale du dossier du conducteur	5
Mode MVR	Compatibilité
Dossier patient, interface	
Mode Admin	Désactivé(e)
Type	None (Aucun)
Congé immédiat	Désactivé(e)
Table d'adresses	
Expiration du délai d'expiration de l'adresse	3000
Ports	
Mode STP	Sous tension
Mode Admin	Sous tension
Mode LACP	Sous tension
Négociation automatique	Sous tension
Vitesse	Automatique
Mode duplex :	Automatique

Table 198 : Commutation des paramètres par défaut des fonctions (A continué)

Nom/paramètre de la fonction	Par défaut
Lien Trap	Sous tension
Taille du cadre	9198
Temps d'anti-rebond	0
Contrôle de flux.	Désactivé(e)
Intervalle de chargement	300
Ports, volets de liaison	
Mode Admin	Désactivé(e)
Nombre maximum	5
Durée	10
Mode Admin de récupération automatique	Désactivé(e)
Intervalle de récupération automatique	300
LAG	
Mode Admin Auto-lag	Sous tension
Mode de hachage global Auto-lag	2 Dest MAC, VLAN, EType, port entrant
Mode profil ABV global Auto-lag	Sous tension
Mode de hachage global non unicast	Adresse MAC/IP source : Sous tension Adresse MAC/IP de destination : Sous tension
Nom lag	ch<n> où n est compris entre 1 et 64
Mode Admin	Sous tension
Mode hachage	2 Dest MAC, VLAN, EType, port entrant
Mode STP	Sous tension
Mode statique	Désactivé(e)
Lien Trap	Désactivé(e)
Mode préférence locale	Désactivé(e)
802.1AS, monde	
État 802.1AS	Désactivé(e)
priority2 de l'horloge locale1:	248
802.1AS, interface	
Mode Admin	Désactivé(e)

Table 198 : Commutation des paramètres par défaut des fonctions (A continué)

Nom/paramètre de la fonction	Par défaut
Seuil Pdelay	3000
Réponses perdues autorisées	3
Intervalle de synchronisation initial	-3
Intervalle Pdelay initial	0
Intervalle d'annonce initial	0
Expiration du délai SyncRx	3
Délai AnnounceRx dépassé	3
MRP, Global	
Mode MVRP	Désactivé(e)
Mode MMRP	Désactivé(e)
Mode MSRP	Désactivé(e)
PDSF taille de l'émetteur-récepteur	Désactivé(e)
Machine d'état périodique (mode MVRP)	Sous tension
Machine d'état périodique (mode MMRP)	Sous tension
PDSF ports d'entrée de ventilateur maximum	0
Propagation des limites du PDSF	Désactivé(e)
PDSF intervalle de temps de transmission PDU	100
Cartographie 802.1qav, globale	
Priorité EAV	Classe A : 3 Classe B 2
Priorité de remappage EAV	Classe A : 0 Classe B 0
MRP, interface	
Mode MVRP	Désactivé(e)
Mode MMRP	Désactivé(e)
Mode MSRP	Désactivé(e)
Rejoindre le minuteur	20
Quitter le minuteur	100
Laisser tous les minuteurs	1000

Table 198 : Commutation des paramètres par défaut des fonctions (A continué)

Nom/paramètre de la fonction	Par défaut
PDSF CLASSE SR PVID	2
Paramètres Qav, interface	
Classe A, PDSF bande passante delta	100
Classe B, PDSF bande passante delta	0
Protection de boucle L2, Global	
Mode Admin	Désactivé(e)
Intervalle annoncé TLV	5
Réception PDU maximale	1
Protection de boucle L2, interface	
Restez en vie	Désactivé(e)
Action RX	Désactivé(e)
Auto-VLAN, Auto-caméra	
Mode Admin, global	Désactivé(e)
Priorité	7
Mode Admin, interface	Désactivé(e)
Auto-VLAN, auto-WiFi	
Mode Admin, global	Désactivé(e)
Priorité	7
Mode Admin, interface	Désactivé(e)

Paramètres par défaut des fonctions de routage, OSPF, OSPFv3 et multicast

Le tableau suivant décrit les paramètres par défaut des fonctionnalités de routage, OSPF, OSPFv3 et multicast que vous pouvez configurer.

(Les paramètres en lecture seule ne sont pas inclus dans le tableau mais peuvent être inclus dans la fiche technique, que vous pouvez télécharger en visitant netgear.com/support/download/.)

Table 199 : Paramètres par défaut des fonctions de routage, OSPF, OSPFv3 et multicast

Nom/paramètre de la fonction	Par défaut
Table de routage, préférence de routage	
Statique	1
RIP	120
OSPF intra	110
OSPF Inter	110
OSPF externe	110
IP, Global	
Mode routage	Sous tension
Réponses d'écho ICMP	64
Redirections ICMP	Désactivé(e)
Intervalle limite de débit ICMP	1000
Taille de rafale limite de débit ICMP	100
Passerelle globale par défaut	Non configuré
IP, interface	
Méthode de configuration de l'adresse IP	None (Aucun)
adresse IP	None (Aucun)
Masque de sous-réseau	None (Aucun)
Mode routage	Désactivé(e)
Mode administratif	Sous tension
Transférer les diffusions dirigées sur le réseau	Désactivé(e)
Type d'encapsulation	Ethernet
ARP proxy	Sous tension
ARP proxy local	Désactivé(e)
Bande passante	Dépend de la capacité du port (La bande passante est attribuée automatiquement, mais vous pouvez modifier informatique.)
Destination ICMP inaccessible	Sous tension

Table 199 : Paramètres par défaut des fonctions de routage, OSPF, OSPFv3 et multicast (A continué)

Nom/paramètre de la fonction	Par défaut
Redirections ICMP	Désactivé(e)
IP MTU	1500
IP, IP secondaire	
Adresse IP secondaire	None (Aucun)
Masque de sous-réseau IP secondaire	None (Aucun)
IPv6, Global	
Routage monodiffusion IPv6	Désactivé(e)
Limite de saut	64
Intervalle d'erreur de limite de débit ICMPv6	1000
Taille de rafale limite de débit ICMPv6	100
IPv6, interface	
Mode IPv6.	Désactivé(e)
Mode client DHCPv6	Désactivé(e)
Mode de configuration automatique d'adresse sans état	Désactivé(e)
Mode routage	Désactivé(e)
Mode Admin	Sous tension
MTU	1500
La détection des adresses dupliquées transmet	1
Intervalle de temps de vie	1800
Intervalle NS ADV	0
Intervalle ADV atteignable	0
Intervalle ADV	600
Indicateur de configuration gérée ADV	Désactivé(e)
ADV autre drapeau CONFIG	Désactivé(e)
Préférence du routeur	Moyen(ne)
Indicateur de suppression ADV	Désactivé(e)
Destination inaccessible	Sous tension
IPv6, préférence d'itinéraire	
Statique	1

Table 199 : Paramètres par défaut des fonctions de routage, OSPF, OSPFv3 et multicast (A continué)

Nom/paramètre de la fonction	Par défaut
OSPFv3 intra	110
OSPFv3 inter	110
Externe OSPFv3	110
ARP, Global	
Durée d'âge	1200
Temps de réponse	1
Nouvelles tentatives	4
Taille des caches	4096
Renouvellement dynamique	Sous tension
RIP, Global	
Mode d'administration RIP	Sous tension
Mode Fractionner horizon	Tranquillité d'esprit
Auto Summary Mode	Désactivé(e)
Mode d'acceptation des routes hôte	Sous tension
Origine des informations par défaut	Désactivé(e)
Métrique par défaut	0
RIP, interface	
Envoyer la version	RIP-2
Version de réception	Les deux
Mode RIP	Désactivé(e)
Type d'authentification	None (Aucun)
ID de clé d'authentification	0
RIP, redistribution de route	
Source	Connecté
Mode redistribution	Désactivé(e)
Métrique	0
Distribuer la liste	0
OSPF, Configuration d'annonce de route par défaut	
Origine des informations par défaut	Désactivé(e)

Table 199 : Paramètres par défaut des fonctions de routage, OSPF, OSPFv3 et multicast (A continué)

Nom/paramètre de la fonction	Par défaut
Toujours	Faux
Métrique	0
Type métrique	Type externe 2
OSPF, Global	
Mode Admin	Sous tension
Code ID du routeur	0.0.0.0
Compatibilité RFC 1583	Sous tension
État LSA opaque	Sous tension
Intervalle de débordement de sortie (s)	0
Délai SPF (s)	5
Temps de maintien SPF (s)	10
Limite LSDB externe	-1
Métrique par défaut	0
Chemins maximum	16
Bande passante de référence autocoûte	100
Paramètre passif par défaut	Désactivé(e)
Interfaces OSPF (configurables)	
ID zone	0
Mode Admin	Désactivé(e)
Priorité du routeur	1
Intervalle de retransmission	5
Intervalle Hello	10
Intervalle mort	40
Intervalle de délai lfransit	1
MTU ignoré	Désactivé(e)
Mode passif	Désactivé(e)
Type de réseau	Diffusion
Type d'authentification	None (Aucun)
OSPF, distribution de route	

Table 199 : Paramètres par défaut des fonctions de routage, OSPF, OSPFv3 et multicast (A continué)

Nom/paramètre de la fonction	Par défaut
Redistribuer (pour toutes les sources)	Désactivé(e)
Métrique (pour toutes les sources)	0
OSPF, NSF OSPF	
Modes pris en charge	Désactivé(e)
Intervalle de redémarrage	120
Mode d'assistance	Toujours
Helper strict LSA vérification	Sous tension
OSPFv3, Configuration d'annonce de route par défaut	
Origine des informations par défaut	Désactivé(e)
Toujours	Faux
Métrique	0
Type métrique	Type externe 2
OSPFv3, Global	
Mode Admin	Sous tension
Code ID du routeur	0.0.0.0
Intervalle de débordement de sortie (s)	0
Limite LSDB externe	-1
Métrique par défaut	0
Chemins maximum	16
Bande passante de référence autocoûte	100
Paramètre passif par défaut	Désactivé(e)
Mode d'assistance	Toujours
Helper strict LSA vérification	Sous tension
OSPFv3, Configuration de l'interface	
ID zone	0
Mode Admin	Désactivé(e)
Priorité du routeur	1
Intervalle de retransmission	5
Intervalle Hello	10

Table 199 : Paramètres par défaut des fonctions de routage, OSPF, OSPFv3 et multicast (A continué)

Nom/paramètre de la fonction	Par défaut
Intervalle mort	40
Intervalle de délai lfrtransit	1
MTU ignoré	Désactivé(e)
Mode passif	Désactivé(e)
Type de réseau	Diffusion
Coût métrique	1
OSPFv3, distribution de route	
Redistribuer (pour toutes les sources)	Désactivé(e)
Métrique (pour toutes les sources)	0
Type de métrique (pour toutes les sources)	Type externe 2
Balise (pour toutes les sources)	0
OSPFv3, NSF OSPF	
Modes pris en charge	Désactivé(e)
Intervalle de redémarrage	120
Découverte du routeur	
Mode publicité	Désactivé(e)
Annoncer l'adresse	224.0.0.1
Intervalle de publicité maximum	600
Intervalle de publicité minimum	450
Annoncez Lifetime	1800
Niveau de préférence	0
VRRP, Global	
Mode Admin	Désactivé(e)
Multidiffusion, Global	
Mode Admin	Désactivé(e)
Multidiffusion, interface	
Seuil TTL	1
Multidiffusion, DVMRP, Global	
Mode Admin	Désactivé(e)

Table 199 : Paramètres par défaut des fonctions de routage, OSPF, OSPFv3 et multicast (A continué)

Nom/paramètre de la fonction	Par défaut
Multicast, DVMRP, interface	
Mode interface	Désactivé(e)
Métrique d'interface	1
Multidiffusion, IGMP, Global	
Mode Admin	Désactivé(e)
Multidiffusion, IGMP, interface de routage	
Mode Admin	Désactivé(e)
Version	V3
Robustesse	2
Intervalle de requête	125
Temps de réponse maximal de la requête	100
Intervalle de requête de démarrage	31
Nombre de requêtes de démarrage	2
Intervalle de requête du dernier membre	10
Nombre de requêtes du dernier membre	2
Multidiffusion, IGMP, interface proxy	
Mode Admin	Désactivé(e)
Intervalle de rapport non sollicité	1
Multidiffusion, PIM, Global	
Mode Admin	Désactivé(e)
Multidiffusion, PIM, interface	
Mode Admin	Désactivé(e)
Intervalle Hello	30
Intervalle de jointure/élagueage	60
Bordure BSR	Désactivé(e)
Priorité DR	1
Multicast, PIM, candidat BSR	
Longueur du masque de hachage	30
Priorité	0

Table 199 : Paramètres par défaut des fonctions de routage, OSPF, OSPFv3 et multicast (A continué)

Nom/paramètre de la fonction	Par défaut
Intervalle d'annonce (s)	60
Multicast IPv6, PIM, Global	
Mode Admin	Désactivé(e)
Multicast IPv6, PIM, interface	
Mode Admin	Désactivé(e)
Intervalle Hello	30
Intervalle de jointure/élaguage	60
Bordure BSR	Désactivé(e)
Priorité DR	1
Multicast IPv6, PIM, candidat BSR	
Longueur du masque de hachage	126
Priorité	0
Intervalle d'annonce	60
Multicast IPv6, MLD, Global	
Mode Admin	Désactivé(e)
Multicast IPv6, MLD, interface de routage	
Mode Admin	Désactivé(e)
Version	V2
Intervalle de requête	125
Temps de réponse maximal de la requête	10000
Intervalle de requête de démarrage	31
Nombre de requêtes de démarrage	2
Intervalle de requête du dernier membre	1000
Nombre de requêtes du dernier membre	2
Multicast IPv6, MLD, interface proxy	
Mode Admin	Désactivé(e)
Intervalle de rapport non sollicité	1

QoS propose les paramètres par défaut

Le tableau suivant décrit les paramètres par défaut des fonctionnalités QoS que vous pouvez configurer.

(Les paramètres en lecture seule ne sont pas inclus dans le tableau mais peuvent être inclus dans la fiche technique, que vous pouvez télécharger en visitant netgear.com/support/download/.)

Table 200 : QoS propose les paramètres par défaut

Nom/paramètre de la fonction	Par défaut
Cos, Global	
Mode confiance globale	Trust IP-DSCP appliqué à toutes les interfaces
Cos, mappage de file d'attente 802.1p.	
priorité 802.1p (802.1p -> file d'attente)	0 -> 1 1 -> 0 2 -> 0 3 -> 1 4 -> 2 5 -> 2 6 -> 3 7 -> 3
Cos, mappage de file d'attente IP DSCP	
Priorité IP DSCP (IP DSCP -> file d'attente)	0 à 7 -> 1 8 à 23 -> 0 24 à 31 -> 1 32 à 47 -> 2 48 à 63 -> 3
Cos, interface	
Mode de confiance de l'interface	IP DSCP
Vitesse de mise en forme de l'interface	0
Cos, file d'attente d'interface	
ID de file d'attente	0
Bande passante minimale	0

Table 200 : QoS propose les paramètres par défaut (A continué)

Nom/paramètre de la fonction	Par défaut
Type de planificateur	Poids
Type de gestion de file d'attente	Chute de queue
Cos, préférence de DROP de file d'attente	
Supprimer le niveau de priorité	1 (pour toutes les interfaces et toutes les files d'attente)
Seuil minimum WRED	40 (pour toutes les interfaces et toutes les files d'attente)
Seuil maximum WRED	100 (pour toutes les interfaces et toutes les files d'attente)
Échelle de probabilité de chute WRED	10 (pour toutes les interfaces et toutes les files d'attente)
DiffServ, Global	
Aucune classe, stratégie et service par défaut n'est configuré	
Mode d'administration DiffServ	Sous tension

Paramètres par défaut des fonctions de sécurité

Le tableau suivant décrit les paramètres par défaut des fonctions de sécurité que vous pouvez configurer.

(Les paramètres en lecture seule ne sont pas inclus dans le tableau mais peuvent être inclus dans la fiche technique, que vous pouvez télécharger en visitant netgear.com/support/download/.)

Table 201 : Paramètres par défaut des fonctions de sécurité

Nom/paramètre de la fonction	Par défaut
Gestion sécurité, utilisateur local, mot de passe utilisateur	
Longueur minimale du mot de passe	8
Expiration du mot de passe (jours)	0
Historique des mots de passe	0
Tentatives de verrouillage	5

Table 201 : Paramètres par défaut des fonctions de sécurité (A continué)

Nom/paramètre de la fonction	Par défaut
Heure de déverrouillage	5
Déverrouiller le mode minuterie	Sous tension
Gestion de la sécurité, utilisateur local, MFA Global	
Mode d'authentification multifacteur	Désactivé(e)
Gestion de la sécurité, Activer le mot de passe	
Type de chiffrement	SHA512
Sécurité de gestion, mot de passe de ligne	
Type de cryptage (Console, Telnet et SSH)	SHA512
Management Security, RADIUS, Global	
Aucun serveur RADIUS configuré	
Interface source	VLAN 1
Nombre maximum de retransmissions	4
Délai d'expiration	5
Mode comptabilité	Désactivé(e)
Mode attribut RADIUS 4	Désactivé(e)
Management Security, TACAS+, Global	
Aucun serveur TACACS+ configuré	
Expiration du délai de connexion.	5
Interface source	VLAN 1
Gestion de la sécurité, liste d'authentification	
Liste des valeurs par défaut	L'option 1 est locale, les options 2 à 6 sont N/A.
Liste des réseaux	L'option 1 est locale, les options 2 à 6 sont N/A.
Gestion de la sécurité, Activer la liste d'authentification	
Liste d'activations	L'option 1 est activée, l'option 2 est aucune, les options 3, 4 et 5 sont N/A.
EnableNetList	L'option 1 est activée, l'option 2 est aucune, les options 3, 4 et 5 sont N/A.
Gestion de la sécurité, liste d'authentification Dot1x	
dot1xList	Désactivé(e)
Gestion de la sécurité, liste d'authentification HTTP	

Table 201 : Paramètres par défaut des fonctions de sécurité (A continué)

Nom/paramètre de la fonction	Par défaut
HttpList	Désactivé(e)
Gestion de la sécurité, liste d'authentification HTTPS	
HttpsList	Désactivé(e)
Accès, HTTP	
Accès HTTP	Sous tension
Port HTTP	49151
Expiration logicielle de session HTTP (minutes)	15
Délai d'attente de session HTTP (heures)	24
Nombre maximal de sessions HTTP	16
Accès, HTTPS	
Accès HTTPS	Désactivé(e)
Port HTTPS	443
Expiration logicielle de session HTTPS (minutes)	15
Délai d'attente de session HTTPS (heures)	24
Nombre maximal de sessions HTTPS	16
Accès, SSH	
Mode administrateur SSH	Désactivé(e)
Expiration de la session SSH	5
Nombre maximal de sessions SSH	5
Liste d'authentification	Liste des réseaux
Activer la liste d'authentification	Liste d'activations
Port SSH	22
Mode d'authentification par clé publique SSH	Désactivé(e)
Mode administrateur du serveur SCP	Désactivé(e)
Nombre maximal de tentatives d'authentification SSH	3
Accès, Telnet, liste d'authentification	
Liste d'authentification	Liste des réseaux
Activer la liste d'authentification	Liste d'activations
Access, Telnet, Telnet entrant	

Table 201 : Paramètres par défaut des fonctions de sécurité (A continué)

Nom/paramètre de la fonction	Par défaut
Mode d'administration du serveur Telnet	Sous tension
Autoriser de nouvelles sessions Telnet	Sous tension
Expiration de session (minutes)	5
Nombre maximum de sessions	5
Access, Telnet, Telnet sortant	
Autoriser de nouvelles sessions Telnet	Sous tension
Expiration de session (minutes)	5
Nombre maximum de sessions	5
Accès, Console	
Délai de connexion au port série (minutes)	5
Débit en bauds (bps)	115200
Liste d'authentification	Liste des valeurs par défaut
Activer la liste d'authentification	Liste d'activations
Accès, déni de service	
Déni de service taille minimale de l'en-tête TCP	20
Déni de service ICMPv4.	Désactivé(e)
Déni de service taille maximale des paquets ICMPv4	512 (si la taille maximale de paquet ICMPv4 est activée)
Déni de service ICMPv6.	Désactivé(e)
Déni de service taille maximale des paquets ICMPv6	512 (si la taille maximale de paquet ICMPv6 est activée)
Premier fragment de déni de service	Désactivé(e)
Fragment ICMP de déni de service	Désactivé(e)
Déni de service SIP=DIP	Désactivé(e)
Déni de service SMAC=DMAC	Désactivé(e)
Déni de service TCP fin & URG & PSH	Désactivé(e)
Drapeau et séquence TCP de déni de service	Désactivé(e)
Fragment TCP de déni de service	Désactivé(e)
Décalage TCP de déni de service	Désactivé(e)
Port TCP de déni de service	Désactivé(e)

Table 201 : Paramètres par défaut des fonctions de sécurité (A continué)

Nom/paramètre de la fonction	Par défaut
Déni de service TCP SYN	Désactivé(e)
Déni de service TCP SYN & fin	Désactivé(e)
Port UDP de déni de service	Désactivé(e)
Mode DROP de balise VLAN0 empilé	Désactivé(e)
Accès, contrôle d'accès, profil d'accès	
Aucun profil d'accès configuré	
Authentification de port, 802.1X, Global	
Mode admin dot1x	Désactivé(e)
Authentification en mode admin	Désactivé(e)
Mode d'affectation VLAN	Désactivé(e)
Mode flood EAPOL	Désactivé(e)
Mode de création de VLAN dynamique	Désactivé(e)
Mode moniteur	Désactivé(e)
Utilisateurs	admin
Connexion	Liste des valeurs par défaut
Authentification de port, 802.1X, interface	
Mode de contrôle	Automatique
Mode hôte	Multi-domaine-Multi-hôte
MAB	Désactivé(e)
Type d'authentification MAB	N/A
Période de silence	60
Période de transmission	30
VLAN invité	0
ID VLAN non authentifié	0
Nombre maximal de demandes de réauthentification	2
Délai d'attente du demandeur	30
Délai d'attente du serveur	30
Nombre maximum de demandes	2
Fonctionnalités de consultation	Authentification

Table 201 : Paramètres par défaut des fonctions de sécurité (A continué)

Nom/paramètre de la fonction	Par défaut
Réauthentification périodique	Désactivé(e)
Type de période de réauthentification	Serveur
Période de réauthentification	0
Nombre maximum d'utilisateurs	48
Ordre d'authentification, méthode 1	DOT1X
Ordre d'authentification, méthode 2	MAB
Ordre d'authentification, méthode 3	Portail captif
Contrôle du trafic, filtre MAC	
Aucun filtre MAC configuré	
Contrôle du trafic, sécurité des ports, Administration des ports	
Mode de sécurité du port	Désactivé(e)
Contrôle du trafic, sécurité des ports, interface	
Mode de sécurité	Désactivé(e)
Nombre maximal d'adresses MAC apprises	4096
Nombre maximal d'adresses MAC statiques	48
Arrêt de violation	Désactivé(e)
Interruption de violation	Désactivé(e)
Contrôle du trafic, Groupe privé	
Groupes privés	Aucun configuré
Contrôle du trafic, port protégé	
Protection des ports	Aucun configuré
Contrôle du trafic, VLAN privé	
VLAN privés	Non configuré
Contrôle du trafic, storm control, monde	
Diffuser storm control All	Sous tension
Multicast storm control All	Désactivé(e)
Monodiffusion storm control All inconnue	Désactivé(e)
Contrôle du trafic, storm control, interface	
Tempête de diffusion, mode récupération	Sous tension

Table 201 : Paramètres par défaut des fonctions de sécurité (A continué)

Nom/paramètre de la fonction	Par défaut
Tempête de diffusion, type de niveau de récupération	pourcentage
Tempête de diffusion, niveau de récupération	5
Tempête de diffusion, action de contrôle	None (Aucun)
Tempête de multidiffusion, mode de récupération	Désactivé(e)
Tempête de multidiffusion, type de niveau de récupération	pourcentage
Tempête de multidiffusion, niveau de récupération	5
Tempête multicast, action de contrôle	None (Aucun)
Tempête unicast, mode récupération	Désactivé(e)
Tempête de monodiffusion, type de niveau de récupération	pourcentage
Tempête unicast, niveau de récupération	5
Tempête unicast, action de contrôle	None (Aucun)
Contrôle, surveillance DHCP, Global	
Mode de surveillance DHCP	Désactivé(e)
Validation de l'adresse MAC	Sous tension
Contrôle, surveillance DHCP, interface	
Mode confiance	Désactivé(e)
Paquets non valides	Désactivé(e)
Limite de débit (PPS)	None (Aucun)
Intervalle de rafale (s)	N/A
Contrôle, surveillance DHCP, persistant	
Magasin	Local
Délai d'écriture	300
Contrôle, surveillance DHCPv6, Global	
Mode de surveillance DHCPv6	Désactivé(e)
Validation de l'adresse MAC	Sous tension
Contrôle, surveillance DHCPv6, interface	
Mode confiance	Désactivé(e)
Paquets non valides	Désactivé(e)

Table 201 : Paramètres par défaut des fonctions de sécurité (A continué)

Nom/paramètre de la fonction	Par défaut
Limite de débit (PPS)	None (Aucun)
Intervalle de rafale (s)	N/A
Contrôle, surveillance DHCPv6, persistant	
Magasin	Local
Délai d'écriture	300
Contrôle, IP source Guard, interface	
Mode IPSG	Désactivé(e)
Sécurité du port IPSG	Désactivé(e)
Contrôle, IPv6 source Guard, interface	
Mode IPv6SG.	Désactivé(e)
Sécurité du port IPv6SG	Désactivé(e)
Contrôle, inspection ARP dynamique, Global	
Validez l'adresse MAC source	Désactivé(e)
Validez l'adresse MAC de destination	Désactivé(e)
Valider IP	Désactivé(e)
Contrôle, inspection ARP dynamique, VLAN	
Identifiant VLAN	1
Mode Admin	Désactivé(e)
Paquets non valides	Sous tension
Indicateur statique	Désactivé(e)
Contrôle, inspection ARP dynamique, interface	
Mode confiance	Désactivé(e)
Limite de débit (PPS)	15
Intervalle de rafale (s)	1
Contrôle, Portail captif, Global	
Mode Admin	Désactivé(e)
Port HTTP supplémentaire	0
Port sécurisé HTTP supplémentaire	0
Expiration du délai d'authentification	300

Table 201 : Paramètres par défaut des fonctions de sécurité (A continué)

Nom/paramètre de la fonction	Par défaut
Contrôle, portail captif, configuration CP	
ID CP	1
Nom du CP	Par défaut
Mode Admin	Sous tension
Protocole	HTTP
Vérification	Invité
Bloc	Non bloqué
Groupe	0
Durée d'inactivité	0
Déconnexion de l'utilisateur	Désactivé(e)
Serveur d'authentification RADIUS	None (Aucun)
Mode redirection	Désactivé(e)
URL de redirection	/v1/security/captive_portal/cp_welcome.html
couleur d'arrière-plan :	#BFBFBF
Couleur de premier plan	#999999
Couleur du séparateur	#B70024
Bande passante maximale réduite	0
Bande passante maximale réduite	0
Entrée maximale	0
Sortie maximale	0
Total maximum	0
Contrôle, portail captif, Groupe CP	
ID du groupe	1
Nom du groupe	Par défaut
Contrôle, portail captif, drapeaux d'interruption CP	
Mode trappe CP	Désactivé(e)
Échec de l'authentification du client	None (Aucun)
client connecté	Désactivé(e)
Base de données client saturée	None (Aucun)

Table 201 : Paramètres par défaut des fonctions de sécurité (A continué)

Nom/paramètre de la fonction	Par défaut
Déconnexion du client	Désactivé(e)
Listes de contrôle d'accès (ACL)	
Aucune liste de contrôle d'accès par défaut configurée	
Nombre total de listes de contrôle d'accès prises en charge	100. Ce nombre total s'applique à toutes les ACL MAC, ACL IPv4 et ACL IPv6.
MAC ACLs	Aucun configuré
Listes de contrôle d'accès IP	Aucun configuré
Listes de contrôle d'accès IPv6	Aucun configuré

Paramètres par défaut des fonctions de surveillance

Le tableau suivant décrit les paramètres par défaut des fonctions de surveillance que vous pouvez configurer.

(Les paramètres en lecture seule ne sont pas inclus dans le tableau mais peuvent être inclus dans la fiche technique, que vous pouvez télécharger en visitant netgear.com/support/download/.)

Table 202 : Paramètres par défaut des fonctions de surveillance

Fonction	Par défaut
Journaux, Journal de mémoire	
Statut Admin	Sous tension
Comportement	Envelopper
Filtre de gravité	Remarque
Seuil	80
Journaux, Journal des commandes	
Statut Admin	Désactivé(e)
Journaux, Journal de la console	
Statut Admin	Désactivé(e)
Filtre de gravité	Erreur

Table 202 : Paramètres par défaut des fonctions de surveillance (A continué)

Fonction	Par défaut
Journaux, Journal du serveur	
Statut Admin	Désactivé(e)
Port UDP local	514
Source nterface	VLAN 1
Journaux, Journal USB	
Mode journal USB	Écraser sur Full
Filtre de gravité	Remarque
Mise en miroir, mise en miroir de plusieurs ports, Global	
ID de session	1
Port de destination	None (Aucun)
Mode Admin	Faux
Type de filtre	None (Aucun)
Mise en miroir, mise en miroir de plusieurs ports, interface	
Direction	None (Aucun)
Mise en miroir, VLAN RSPAN	
Identifiant VLAN	1
Mode Admin	Faux
Mise en miroir, commutateur source RSPAN, Global	
ID de session	1
Mode Admin	Faux
VLAN de destination RSPAN	None (Aucun)
Type de filtre	None (Aucun)
Mise en miroir, commutateur source RSPAN, interface	
Direction	None (Aucun)
Mise en miroir, commutateur de destination RSPAN, Global	
ID de session	1
Mode Admin	Faux
VLAN source RSPAN	None (Aucun)
Port de destination RSPAN	None (Aucun)

Table 202 : Paramètres par défaut des fonctions de surveillance (A continué)

Fonction	Par défaut
Type de filtre	None (Aucun)
Agent sFlow	
Interface source	VLAN 1
Récepteur SFlow	
Délai d'attente du récepteur	0
Pas de délai d'attente	Faux
Taille maximale du datagramme	1400
Adresse du récepteur	0.0.0.0
Port récepteur	6343
Interface sFlow	
Poller, index du récepteur	0
Poller, intervalle Poller	0
ECHANTILLONNEUR, index récepteur	0
Échantillonneur, fréquence d'échantillonnage	0
Échantillonneur, taille maximale de la barre de coupe	128

Spécifications techniques générales du matériel

Les spécifications techniques matérielles suivantes s'appliquent à tous les modèles de commutateurs de la série M4350 :

Table 203 : Spécifications techniques matérielles générales pour les modèles de commutateurs de la série M4350

Fonction	Description
Température de fonctionnement	Modèles PoE+ et PoE++ : 0 à 40 °C (32 à 104 °F)
	Modèles autres que PoE : 0 à 45 °C (32 à 113 °F)
Humidité de fonctionnement	90 % d'humidité relative maximum, sans condensation

Table 203 : Spécifications techniques matérielles générales pour les modèles de commutateurs de la série M4350 (A continué)

Fonction	Description
Altitude de fonctionnement :	3 000 m maximum
Température de stockage	-4° à 158°F (-20° à 70°C)
Hygrométrie de stockage	95 % d'humidité relative maximum, sans condensation
Altitude de stockage :	3 000 m maximum
Émissions électromagnétiques et certifications d'immunité	CE Classe A, en 55032 : 2015 A11 : 2020, EN 55035 : 2017, EN 61000-3-2:2014, EN 61000-3-3:2013
	VCCI VCCI 32-1, classe A.
	RCM AS/NZS CISPR 32 : 2015+A1:2020, classe B.
	FCC 47 CFR FCC Part 15, SubpartB, Class A; ANSI C63.4: 2014
	ISED : ICES-003 : Question 7, classe A.
	BSMI CNS 15936, classe A.
Certifications de sécurité	EN 62368-1 : 2014/AC:2015 ; IEC 62368-1:2018 2018
	CAN/CSA C22.2 NO. 62368-1 :19, ANSI/UL 62368-1 3e éd.

Spécifications techniques matérielles spécifiques au modèle

Les tableaux des sections suivantes décrivent les principales caractéristiques techniques du matériel pour chaque modèle.

Pour plus d'informations, reportez-vous au manuel de l'utilisateur, que vous pouvez télécharger en vous rendant sur le site www.netgear.fr/support/download.

M4350-8X8F (SKU XSM4316)

Le tableau suivant indique les spécifications spécifiques au modèle M4350-8x8F.

Table 204 : Caractéristiques techniques du matériel pour le modèle M4350-8x8F

Fonction		Description
Interfaces réseau		Huit ports Ethernet 10G/5G/2.5G/1G/100M. Ports 1 Gigabit/10 Gigabit SFP+ (fibre)
Prise d'alimentation CA		100-240 V ~ 50/60 Hz, 3 A
Consommation électrique	Charge max	81,1 W
	Veille	30,5 W
Dimensions	Largeur	220 mm (8,66 po)
	Hauteur	1,70 po (43,2 mm), 1U.
	Profondeur	400 mm (15,75 po)
Poids		4,05kg (8,93lb)

M4350-12X12F (SKU XSM4324)

Le tableau suivant indique les spécifications spécifiques au modèle M4350-12x12F.

Table 205 : Caractéristiques techniques du matériel pour le modèle M4350-12x12F

Fonction		Description
Interfaces réseau		Douze ports Ethernet 10G/5G/2.5G/1G/100M. Ports 1 Gigabit/10 Gigabit SFP+ (fibre)
Prise d'alimentation CA		100-240 V ~ 50/60 Hz, 3 A
Consommation électrique	Charge max	95,8 W
	Veille	34 W
Dimensions	Largeur	220 mm (8,66 po)
	Hauteur	1,70 po (43,2 mm), 1U.
	Profondeur	400 mm (15,75 po)
Poids		4,3kg (9,48lb)

M4350-24G4XF (SKU GSM4328)

Le tableau suivant indique les spécifications spécifiques au modèle M4350-24G4XF.

Table 206 : Spécifications techniques matérielles pour le modèle M4350-24G4XF

Fonction		Description
Interfaces réseau		Vingt-quatre ports Ethernet PoE+ 1G/100M. Ports 1 Gigabit/10 Gigabit SFP+ (fibre)
Prise d'alimentation CA		100-240 V ~ 50/60 Hz, 10 A
Consommation électrique	Max. PoE	792,1 W
	Aucune alimentation PoE	80 W
		32 W
	Veille	
Budget PoE, alimentation interne		648 W
Dimensions	Largeur	440 mm (17,32 po)
	Hauteur	1,70 po (43,2 mm), 1U.
	Profondeur	400 mm (15,75 po)
Poids		6,41kg (14,13lb)

M4350-48G4XF (SKU GSM4352)

Le tableau suivant indique les spécifications spécifiques au modèle M4350-48G4XF.

Table 207 : Caractéristiques techniques du matériel pour le modèle M4350-48G4XF

Fonction		Description
Interfaces réseau		Quarante-huit ports Ethernet PoE+ 1G/100M. Ports 1 Gigabit/10 Gigabit SFP+ (fibre)
Prise d'alimentation CA		100-240 V ~ 50/60 Hz, 10 A
Consommation électrique	Max. PoE	384 W
	Aucune alimentation PoE	99 W
		48,5 W
	Veille	
Budget PoE, alimentation interne		236 W
Dimensions	Largeur	440 mm (17,32 po)
	Hauteur	1,70 po (43,2 mm), 1U.
	Profondeur	400 mm (15,75 po)
Poids		7,19kg (15,85lb)

M4350-24X4V (SKU XSM4328CV)

Le tableau suivant indique les spécifications spécifiques au modèle M4350-24X4V.

Table 208 : Spécifications techniques du matériel pour le modèle M4350-24X4V

Fonction		Description
Interfaces réseau		Vingt-quatre ports Ethernet PoE+ 10G/5G/2.5G/1G/100M. Quatre ports fibre optique SFP28 25G/10G/1G.
Prise d'alimentation CA		100-240 V ~ 50/60 Hz, 10 A
Consommation électrique	Max. PoE	750,1 W
	Aucune alimentation PoE	119,4 W
		53,6 W
	Veille	
Budget PoE, alimentation interne		576 W
Dimensions	Largeur	440 mm (17,32 po)
	Hauteur	1,70 po (43,2 mm), 1U.
	Profondeur	400 mm (15,75 po)
Poids		6,58kg (14,51lb)

M4350-24F4V (SKU XSM4328FV)

Le tableau suivant indique les spécifications spécifiques au modèle M4350-24F4V.

Table 209 : Spécifications techniques du matériel pour le modèle M4350-24F4V

Fonction		Description
Interfaces réseau		Vingt-quatre ports fibre optique 1G/10G SFP+ Quatre ports fibre optique SFP28 25G/10G/1G.
Prise d'alimentation CA		100-240 V ~ 50/60 Hz, 3 A
Consommation électrique	Charge max	119,3 W
	Veille	45,2 W
Dimensions	Largeur	440 mm (17,32 po)
	Hauteur	1,70 po (43,2 mm), 1U.
	Profondeur	400 mm (15,75 po)
Poids		6,25kg (13,78lb)

M4350-44M4X4V (SKU MSM4352)

Le tableau suivant indique les spécifications spécifiques au modèle M4350-44M4X4V.

Table 210 : Spécifications techniques du matériel pour le modèle M4350-44M4X4V

Fonction		Description
Interfaces réseau		Quarante-quatre ports Ethernet PoE++ 2.5G/1G/100M. Quatre ports Ethernet PoE++ 10G/5G/2.5G/1G/100M. Quatre ports fibre optique SFP28 25G/10G/1G.
Prise d'alimentation CA		100-240 V ~ 50/60 Hz, 10 A
Consommation électrique	Max. PoE	351,5 W
	Aucune alimentation PoE	133,5 W
		56,5 W
	Veille	
Budget PoE, alimentation interne		194 W
Dimensions	Largeur	440 mm (17,32 po)
	Hauteur	1,70 po (43,2 mm), 1U.
	Profondeur	400 mm (15,75 po)
Poids		7,34kg (16,18lb)

M4350-36X4V (SKU XSM4340CV)

Le tableau suivant indique les spécifications spécifiques au modèle M4350-36X4V.

Table 211 : Spécifications techniques du matériel pour le modèle M4350-36X4V

Fonction		Description
Interfaces réseau		Trente-six ports Ethernet PoE++ 10G/5G/2.5G/1G/100M. Quatre ports fibre optique SFP28 25G/10G/1G.
Prise d'alimentation CA		100-240 V ~ 50/60 Hz, 12 A
Consommation électrique	Max. PoE	454 W
	Aucune alimentation PoE	148 W
		59,3 W
	Veille	
Budget PoE, alimentation interne		280 W

Table 211 : Spécifications techniques du matériel pour le modèle M4350-36X4V (A continué)

Fonction	Description	
Dimensions	Largeur	440 mm (17,32 po)
	Hauteur	1,70 po (43,2 mm), 1U.
	Profondeur	400 mm (15,75 po)
Poids	7,33kg (16,16lb)	

M4350-24X8F8V (SKU XSM4340V)

Le tableau suivant indique les spécifications spécifiques au modèle M4350-24X8F8V.

Table 212 : Spécifications techniques du matériel pour le modèle M4350-24X8F8V

Fonction	Description	
Interfaces réseau	Vingt-quatre ports Ethernet PoE++ 10G/5/2.5G/1G/100M. Huit ports fibre optique 10G/1G SFP+ Huit ports fibre optique SFP28 25G/10G/1G.	
Prise d'alimentation CA	100-240 V ~ 50/60 Hz, 12 A	
Consommation électrique	Max. PoE	464 W
	Aucune alimentation PoE	151,8 W
		53,4 W
	Veille	
Budget PoE, alimentation interne	290 W	
Dimensions	Largeur	440 mm (17,32 po)
	Hauteur	1,70 po (43,2 mm), 1U.
	Profondeur	400 mm (15,75 po)
Poids	7,24kg (15,96lb)	

M4350-32F8V (SKU XSM4340FV)

Le tableau suivant indique les spécifications spécifiques au modèle M4350-32F8V.

Table 213 : Spécifications techniques du matériel pour le modèle M4350-32F8V

Fonction		Description
Interfaces réseau		Trente-deux ports fibre optique 10G/1G SFP+ Huit ports fibre optique SFP28 25G/10G/1G.
Prise d'alimentation CA		100-240 V ~ 50/60 Hz, 12 A
Consommation électrique	Charge max	156,4 W
	Veille	42,6 W
Dimensions	Largeur	440 mm (17,32 po)
	Hauteur	1,70 po (43,2 mm), 1U.
	Profondeur	400 mm (15,75 po)
Poids		6,95kg (15,32lb)

M4350-16V4C (SKU VSM4320C)

Le tableau suivant indique les spécifications spécifiques au modèle M4350-16V4C.

Table 214 : Spécifications techniques du matériel pour le modèle M4350-16V4C

Fonction		Description
Interfaces réseau		Seize ports fibre optique SFP28 25G/10G/1G. Quatre ports fibre optique QSFP28 40G/100G
Prise d'alimentation CA		100-240 V ~ 50/60 Hz, 12 A
Consommation électrique	Charge max	143,4 W
	Veille	60,4 W
Dimensions	Largeur	440 mm (17,32 po)
	Hauteur	1,70 po (43,2 mm), 1U.
	Profondeur	400 mm (15,75 po)
Poids		7,15kg (15,77lb)

M4350-40X4C (SKU XSM4344C)

Le tableau suivant indique les spécifications spécifiques au modèle M4350-40X4C.

Table 215 : Spécifications techniques du matériel pour le modèle M4350-40X4C

Fonction		Description
Interfaces réseau		Quarante ports Ethernet PoE++ 10G/5G/2.5G/1G/100M. Quatre ports fibre optique QSFP28 40G/100G
Prise d'alimentation CA		100-240 V ~ 50/60 Hz, 12 A
Consommation électrique	Max. PoE	413 W
	Aucune alimentation PoE	200,4 W
		98,8 W
	Veille	
Budget PoE, alimentation interne		196 W
Dimensions	Largeur	440 mm (17,32 po)
	Hauteur	1,70 po (43,2 mm), 1U.
	Profondeur	400 mm (15,75 po)
Poids		7,76kg (17,11lb)