Manuel utilisateur

Allen-Bradley

Switchs Ethernet administrables Stratix 5700

Allen-Bradley • Rockwell Software

Rockwell Automation

Informations importantes destinées à l'utilisateur

Lisez ce document et les documents énumérés dans la section documentations connexes sur l'installation, la configuration et le fonctionnement de cet équipement avant d'installer, de configurer, d'utiliser ou de maintenir ce produit. Les utilisateurs sont tenus de se familiariser avec les instructions d'installation et de câblage, et de respecter tous les codes, lois et normes en vigueur.

Les interventions comme l'installation, le réglage, la mise en service, l'utilisation, le montage, le démontage et la maintenance doivent être assurées par du personnel convenablement formé, conformément au code de pratique en vigueur.

Si cet équipement n'est pas utilisé selon les préconisations du fabricant, la protection fournie par l'équipement peut être altérée.

La société Rockwell Automation, Inc. ne saurait en aucun cas être tenue pour responsable ni être redevable des dommages indirects ou consécutifs liés à l'utilisation ou à l'application de cet équipement.

Les exemples et schémas contenus dans ce manuel sont présentés à titre indicatif seulement. En raison du nombre important de variables et d'impératifs associés à chaque installation, la société Rockwell Automation, Inc. ne saurait être tenue pour responsable ni être redevable des suites d'une utilisation réelle basée sur les exemples et schémas présentés dans ce manuel.

La société Rockwell Automation, Inc. décline également toute responsabilité en matière de propriété intellectuelle et industrielle concernant l'utilisation des informations, circuits, équipements ou logiciels décrits dans ce manuel.

Toute reproduction totale ou partielle du présent manuel sans autorisation écrite de la société Rockwell Automation, Inc. est interdite.

Des remarques sont utilisées tout au long de ce manuel pour attirer votre attention sur les mesures de sécurité à prendre en compte.

	**AVERTISSEMENT :** identifie des actions ou situations susceptibles de provoquer une explosion en environnement dangereux et risquant d'entraîner des blessures pouvant être mortelles, des dégâts matériels ou des pertes financières.
	**ATTENTION :** identifie des actions ou situations risquant d'entraîner des blessures pouvant être mortelles, des dégâts matériels ou des pertes financières. Les messages « Attention » vous aident à identifier un danger, à éviter ce danger et en discerner les conséquences.
IMPORTANT	Informations particulièrement importantes dans le cadre de l'utilisation et de la compréhension du produit.

Des étiquettes peuvent également se situer sur ou à l'intérieur de l'équipement afin de fournir des précautions spécifiques.

	**DANGER D'ÉLECTROCUTION :** l'étiquette ci-contre, placée sur l'équipement ou à l'intérieur (un variateur ou un moteur, par ex.), signale la présence éventuelle de tensions électriques dangereuses.
	**RISQUE DE BRÛLURE :** l'étiquette ci-contre, placée sur l'équipement ou à l'intérieur (un variateur ou un moteur, par ex.) indique que certaines surfaces peuvent atteindre des températures particulièrement élevées.
	**RISQUE D'ARC ÉLECTRIQUE :** l'étiquette ci-contre, placée sur l'équipement ou à l'intérieur (un centre de commande de moteurs, par ex.) indique un risque d'arc électrique. Les arcs électriques provoquent des blessures graves voire mortelles. Veuillez porter un équipement de protection individuelle (EPI) approprié. Respectez TOUTES les exigences réglementaires concernant les pratiques de travail sécuritaires et l'équipement de protection individuelle (EPI).

Ce manuel contient des informations nouvelles et actualisées.

Informations nouvelles et actualisées

Ce tableau répertorie les changements apportés dans cette révision.

Sujet	Page
Mise à jour des exigences matérielles et logicielles de Device Manager	24, 51
Nouvelle fenêtre Express Setup	53, 54
Nouveau processus d'activation du routage	92
Nouvelle interface Internet de Device Manager	95…161

Notes :

Fonctionnalités logicielles du switch

Chapitre 3

Gestion du switch via l'interface Internet de Device Manager

Chapitre 4

Chapitre 5

Gestion du switch via l'environnement Studio 5000

Chapitre 6

Dépannage du switch

Annexe A

Types de données définis par le module

Annexe B

Affectations de port pour les données CIP

Annexe C

Annexe D

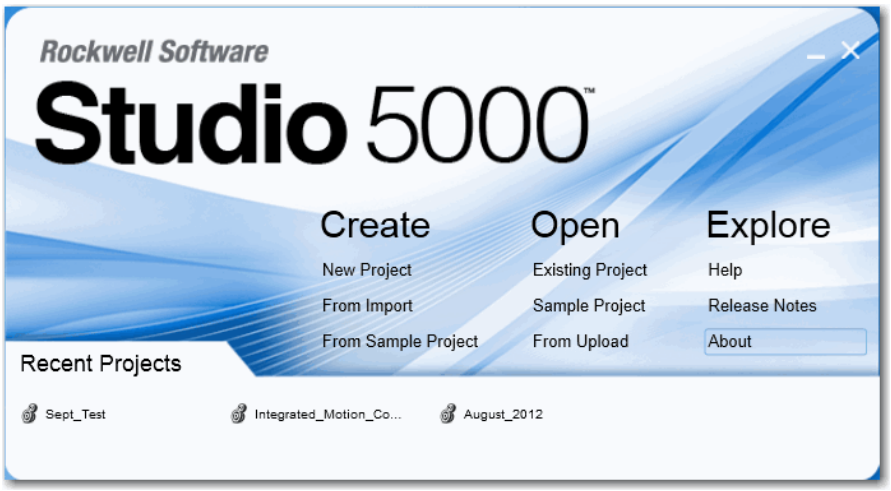
Cette publication décrit les fonctionnalités logicielles embarquées et les outils pour la configuration et la gestion des switchs Ethernet administrables Stratix 5700™. En outre, cette publication fournit des informations de dépannage pour vous aider à résoudre les problèmes de base liés aux switchs et au réseau.

Utilisez ce manuel si vous devez configurer ou surveiller des switchs Ethernet administrables Stratix 5700. Ce guide suppose que vous possédez les connaissances suivantes :

- Connaissances fondamentales sur les switchs en réseau local (LAN)
- Concepts et terminologie du protocole Ethernet et de la mise en réseau local

Environnement Studio 5000

L'environnement d'Ingénierie et de Conception Studio 5000 associe ingénierie et éléments de conception dans un environnement commun. L'application Logix Designer constitue le premier élément de l'environnement Studio 5000. L'application Logix Designer est la nouvelle appellation commerciale du logiciel Logix™ 5000, produit permettant de programmer les automates Logix5000™ pour les solutions de commande discrète, de procédé, de traitement par lot, de mouvement, de sécurité et de variateurs.

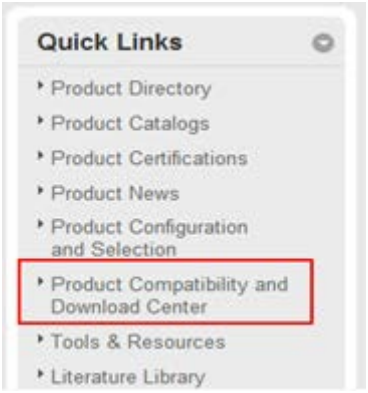


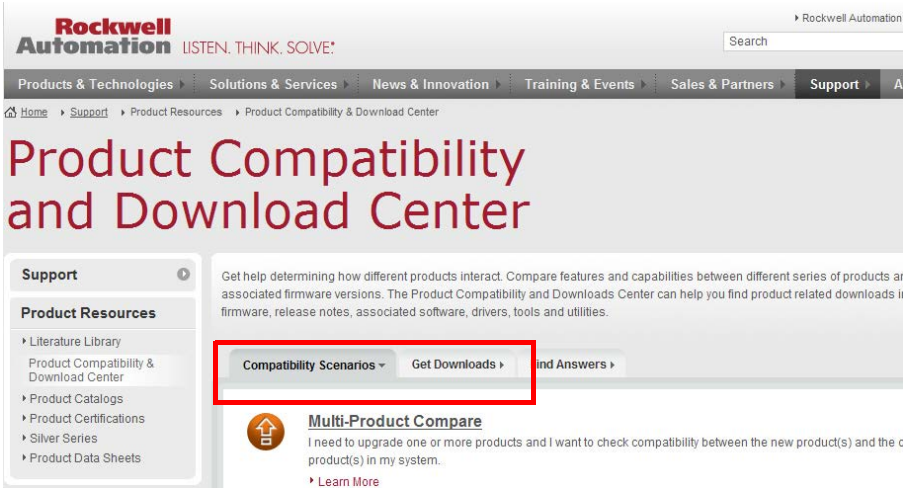
L'environnement Studio 5000 constitue la base des futurs outils et capacités de conception d'ingénierie de Rockwell Automation®. Cet environnement est le seul outil nécessaire aux ingénieurs de conception pour le développement de tous les éléments de leur système de commande.

Accès aux mises à jour produit

Les mises à jour produit sont disponibles en ligne au sein du centre de compatibilité et de téléchargement des produits.

1. Dans la liste des Liens rapides sur http://www.ab.com, choisissez Product Compatibility and Download Center (Centre de compatibilité et de téléchargement produit).





2. Choisissez votre produit depuis les onglets Compatibility Scenarios (Scénarios de compatibilité) ou Get Downloads (Obtenir les téléchargements).

3. Cliquez sur l'icône de téléchargement  pour accéder aux mises à jour produit.

Documentations connexes

Ces documents contiennent des informations complémentaires relatives aux produits connexes de Rockwell Automation.

Documentation	Description
Stratix Ethernet Managed Switches Technical Data, publication 1783-TD001	Fournit des renseignements sur les caractéristiques des switchs.
Ethernet Design Considerations Reference Manual, publication ENET-RM002	Fournit des informations sur la mise en œuvre d'un système basé sur la plate-forme EtherNet/IP.
Aide en ligne de l'interface Internet de Device Manager (fourni avec le switch)	Fournit des informations contextuelles sur la configuration et l'utilisation du switch, y compris les messages système.
Industrial Automation Wiring and Grounding Guidelines, publication 1770-4.1	Fournit des directives générales relatives à l'installation d'un système industriel Rockwell Automation.
Site Internet de certification des produits, http://www.ab.com	Fournit des déclarations de conformité, des certificats et autres détails connexes.

Vous pouvez visualiser ou télécharger les publications depuis l'adresse http://www.rockwellautomation.com/literature/. Pour commander des exemplaires imprimés de documentation technique, contactez votre agence commerciale Rockwell Automation ou votre distributeur Allen-Bradley local.

Pour plus d'informations sur les fonctionnalités supplémentaires du logiciel ou pour aller plus loin dans la configuration, consultez les publications Cisco suivantes à l'adresse http://www.Cisco.com :

- Manuel de référence de la ligne de commande Cisco IE-2000
- Guide de configuration du logiciel Cisco IE-2000
- Guide des Message système du switch Cisco IE-2000

Notes :

À propos des switchs

Les switchs Ethernet administrés Stratix 5700 fournissent une infrastructure de commutation sécurisée pour les environnements difficiles. Ces switchs peuvent être connectés à des périphériques réseau tels que des serveurs, des routeurs et d'autres switchs. Dans les environnements industriels, vous pouvez connecter des périphériques de communication industriels compatibles Ethernet, y compris des automates programmables (PLC), des interfaces homme-machine (IHM), des variateurs, des capteurs et des dispositifs d'E/S.

Références de switch

Ces switchs Stratix 5700 sont disponibles avec un firmware complet ou allégé.

Référence	Description
1783-BMS06SL	Switch administré à 6 ports (4 ports Ethernet, 2 emplacements SFP), firmware allégé
1783-BMS06SA	Switch administré à 6 ports (4 ports Ethernet, 2 emplacements SFP), firmware complet
1783-BMS06TL	Switch administré à 6 ports (6 ports Ethernet), firmware allégé
1783-BMS06TA	Switch administré à 6 ports (6 ports Ethernet), firmware complet
1783-BMS06SGL	Switch administré à 6 ports (4 ports Ethernet ; 2 connecteurs SFP Gigabit), firmware allégé
1783-BMS06SGA	Switch administré à 6 ports (4 ports Ethernet ; 2 connecteurs SFP Gigabit) ; firmware complet
1783-BMS06TGL	Switch administré à 6 ports (4 ports Ethernet ; 2 ports Gigabit) ; firmware complet
1783-BMS06TGA	Switch administré à 6 ports (4 ports Ethernet ; 2 ports Gigabit) ; firmware complet
1783-BMS10CL	Switch administré à 10 ports (8 ports Ethernet, 2 ports mixtes), firmware allégé
1783-BMS10CA	Switch administré à 10 ports (8 ports Ethernet, 2 ports mixtes), firmware complet
1783-BMS10CGL	Switch administré à 10 ports (8 ports Ethernet ; 2 ports mixtes Gigabit) ; firmware complet
1783-BMS10CGA	Switch administré à 10 ports (8 ports Ethernet ; 2 ports mixtes Gigabit) ; firmware complet
1783-BMS10CGN	Switch administré à 10 ports (8 ports Ethernet ; 2 ports mixtes Gigabit) ; firmware complet ; correction d'adresse réseau (NAT)
1783-BMS10CGP	Switch administré à 10 ports (8 ports Ethernet, 2 ports mixtes Gigabit), firmware complet, protocole de synchronisation temporelle (PTP)
1783-BMS12T4E2CGNK	Switch administré à 18 ports (12 ports Ethernet, 4 ports PoE/PoE+, 2 ports mixtes Gigabit), firmware complet, NAT, revêtement enrobant
1783-BMS12T4E2CGP	Switch administré à 18 ports (12 ports Ethernet, 4 ports PoE/PoE+, 2 ports mixtes Gigabit), firmware complet, PTP
1783-BMS12T4E2CGL	Switch administré à 18 ports (12 ports Ethernet, 4 ports PoE/PoE+, 2 ports mixtes Gigabit), firmware allégé
1783-BMS20CL	Switch administré à 20 ports (16 ports Ethernet, 2 emplacements SFP, 2 ports mixtes), firmware allégé
1783-BMS20CA	Switch administré à 20 ports (16 ports Ethernet, 2 emplacements SFP, 2 ports mixtes), firmware complet
1783-BMS20CGL	Switch administré à 20 ports (16 ports Ethernet, 2 emplacements SFP, 2 ports mixtes Gigabit), firmware allégé
1783-BMS20CGN	Switch administré à 20 ports (16 ports Ethernet, 2 emplacements SFP, 2 ports mixtes Gigabit), firmware complet, NAT
1783-BMS20CGP	Switch administré à 20 ports (16 ports Ethernet, 2 emplacements SFP, 2 ports mixtes Gigabit), firmware complet, PTP
1783-BMS20CGPK	Switch administré à 20 ports (16 ports Ethernet, 2 emplacements SFP, 2 ports mixtes Gigabit), firmware complet, PTP, revêtement enrobant
Modules SFP	
1783-SFP100FX	Émetteur-récepteur à fibre optique multimode 100BASE-FX
1783-SFP1GSX	Émetteur-récepteur à fibre optique multimode 1000BASE-SX
1783-SFP100LX	Émetteur-récepteur à fibre optique mode simple 100BASE-LX
1783-SFP1GLX	Émetteur-récepteur à fibre optique mode simple 1000BASE-LX
Alimentation	
Série 1606-XL (recommandée) Série 1606-XLP (recommandée) ou équivalent	Alimentations de classe 2 à sortie 24 V c.c.
Carte SD	
1784-SD1	Carte SD industrielle de 1 Go

Fonctionnalités logicielles du switch

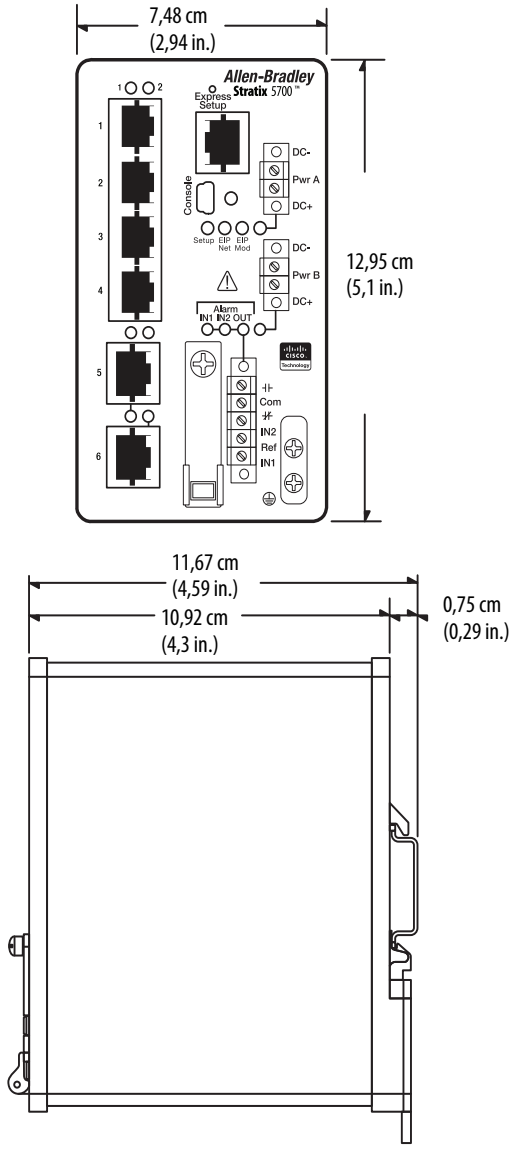
Ces fonctionnalités logicielles sont disponibles avec les switchs Stratix 5700.

Fonctionnalité	Firmware allégé	Firmware complet
CIP Sync (IEEE 1588)		Option séparée
Protocole REP (Resilient Ethernet Protocol)	•	•
FlexLinks		•
Qualité du service (QoS)		•
STP, RSTP, MST (instances)	64	128
Surveillance et interrogation IGMP	•	•
VLAN avec agrégation de ports	64	255
EtherChannel (agrégation de liaisons)		•
Seuil de port (contrôle des tempêtes et lissage de trafic)		•
Prise en charge de IPv6		•
Listes de contrôle d'accès (ACL)		•
Routage statique et interVLAN		•
Contrôle de port CIP et détection des défauts	•	•
Sécurité de port MAC ID		•
Sécurité IEEE 802.1x		•
Authentification TACACS+, RADIUS	•	•
Cryptage (SSH, SNMPv3, HTTPS)		Firmware IOS distinct disponible comme un élément distinct du catalogue
Mise en miroir de ports	•	•
Syslog	•	•
Surveillance de rupture de câble	•	•
Détection d'adresse IP en double		•
SNMP	•	•
Smartports	•	•
DHCP par port	•	•
Interface de ligne de commande (CLI)	•	•
Compatible avec les outils de Cisco : Cisco Network Assistant (CNA) ; CiscoWorks	•	•
Interface EtherNet/IP (CIP)	•	•
Conversion des adresses réseau (NAT)		Option séparée

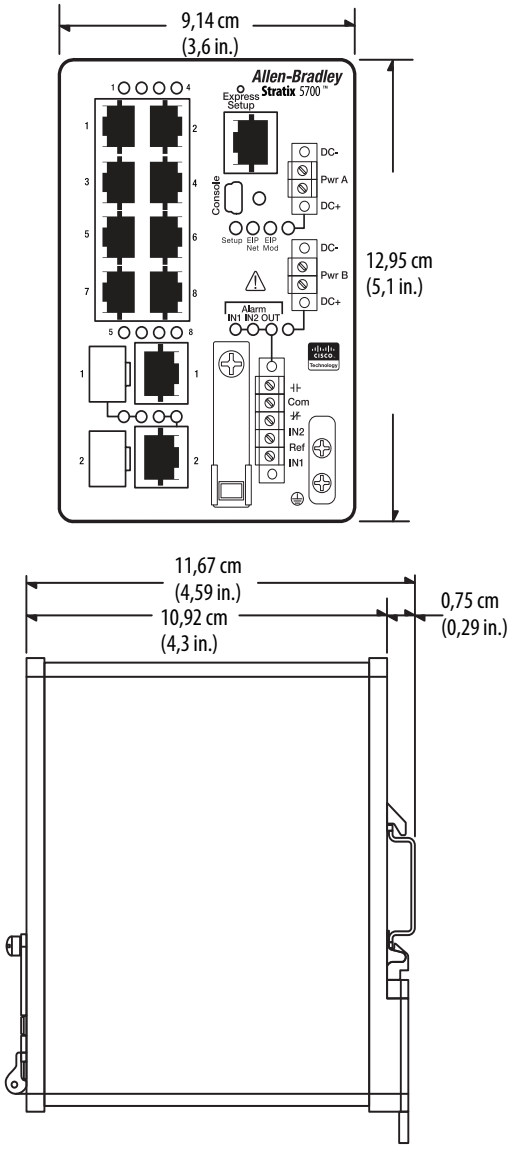
Dimensions du switch

Les schémas suivants représentent les switchs Stratix 5700. Les faces avant réelles varient en fonction de la référence.

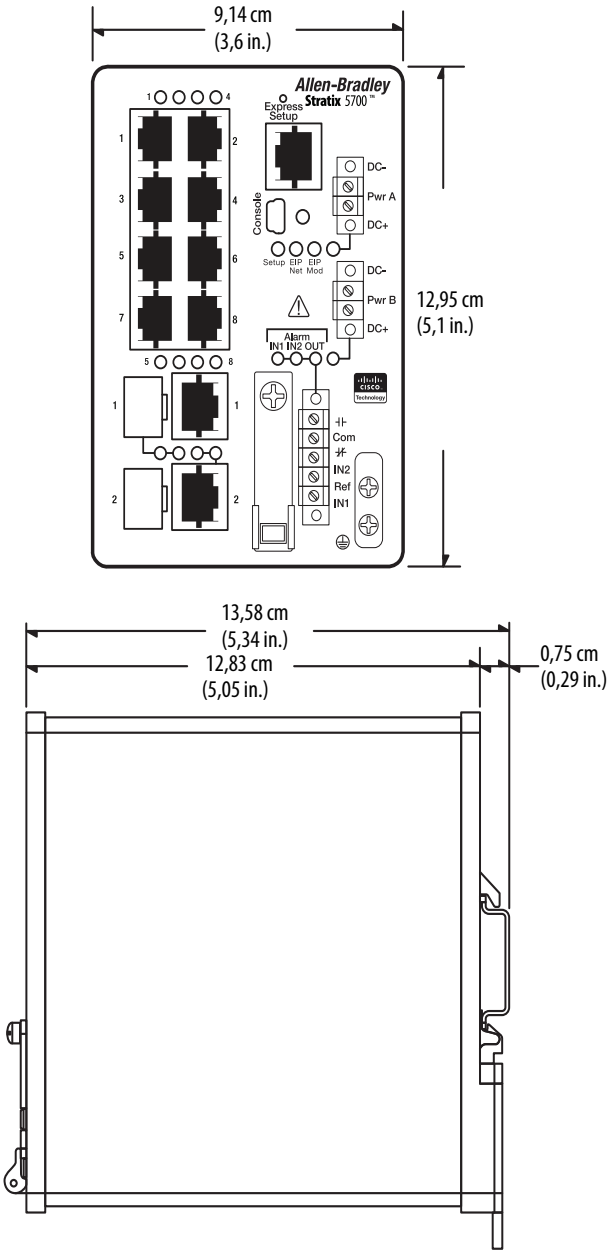
Switchs à 6 ports
1783-BMS06SL, 1783-BMS06SA, 1783-BMS06TL, 1783-BMS06TA, 1783-BMS06SGL, 1783-BMS06SGA, 1783-BMS06TGL, 1783-BMS06TGA



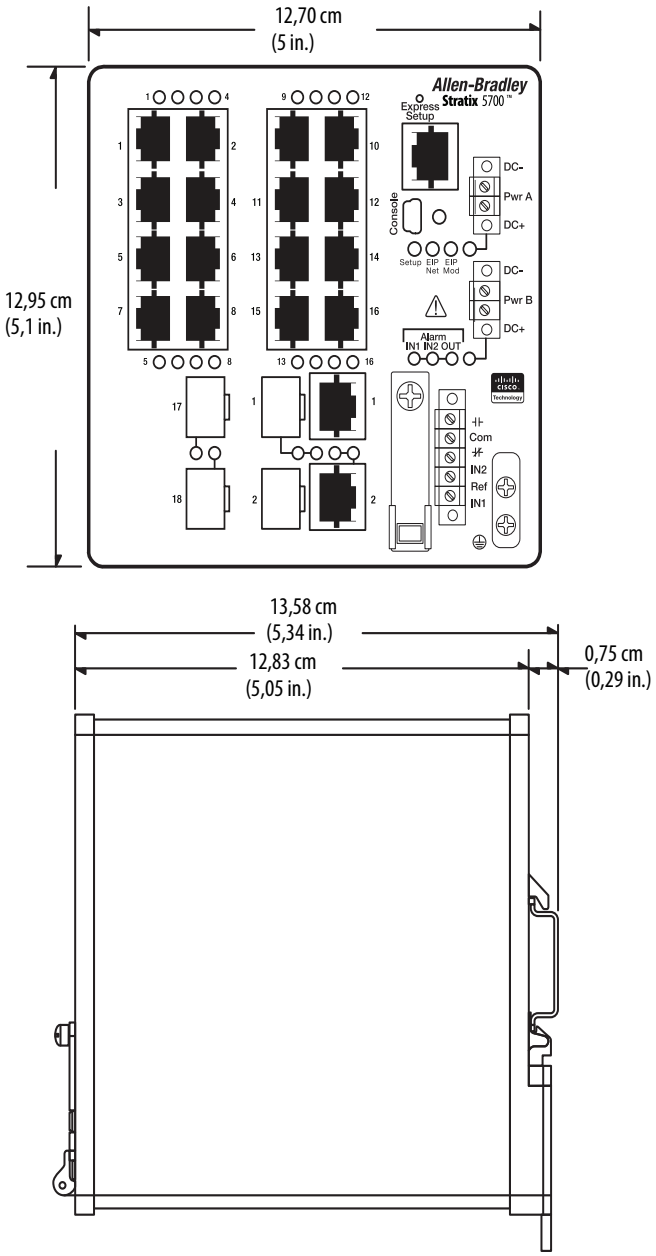
Switchs à 10 ports
1783-BMS10CL, 1783-BMS10CA, 1783-BMS10CGL, 1783-BMS10CGA



Switch à 10 ports
1783-BMS10CGP, 1783-BMS10CGN

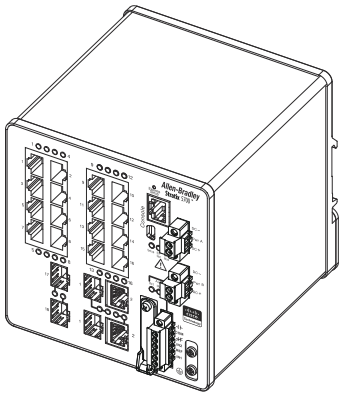


Switchs à 18 et 20 ports
1783-BMS12T4E2CGNK, 1783-BMS12T4E2CGP, 1783-BMS12T4E2CGL, 1783-BMS20CL, 1783-BMS20CA, 1783-BMS20CGL, 1783-BMS20CGP, 1783-BMS20CGN, 1783-BMS20CGPK



Face avant du switch

La face avant du switch comporte les ports, les voyants d'état et les connecteurs d'alimentation et de relais.



Fonctionnalités matérielles du switch

Les caractéristiques matérielles qui suivent sont disponibles sur les switchs Stratix 5700.

Fonctionnalité	Description
Connecteurs d'alimentation et de relais	L'alimentation c.c. et les signaux d'alarme sont reliés au switch par le biais des deux connecteurs en face avant. Un connecteur fournit l'alimentation c.c. principale (Pwr A) et un deuxième connecteur (Pwr B) fournit l'alimentation secondaire. Les deux connecteurs sont physiquement identiques et se trouvent sur le côté droit de la face avant. Le connecteur d'alarme à 6 broches fournit une interface pour un relais de sortie d'alarme et deux entrées d'alarme. La sortie d'alarme peut être activée pour les conditions environnementales, d'alimentation et d'état de port, et peut être configurée pour indiquer une alarme avec un contact normalement ouvert et un contact normalement fermé (forme C). L'interface de ligne de commande vous permet de configurer la sortie d'alarme de manière à être normalement sous tension ou normalement hors tension. Les bornes d'entrée d'alarme peuvent être utilisées pour activer des alarmes pour toutes les conditions externes au switch. Le switch peut fonctionner avec une seule alimentation électrique ou avec une double alimentation électrique. Lorsque les deux sources d'alimentation sont opérationnelles, le switch s'alimente depuis la source c.c. possédant la tension la plus élevée. Si l'une des deux sources d'alimentation tombe en panne, l'autre continue à alimenter le switch.
Port de la console	Pour la configuration, la surveillance et la gestion du switch, vous pouvez connecter un switch à un ordinateur via le port de la console et un câble adaptateur RJ45/DB-9 ou un câble mini USB (aucun de ces câbles n'est fourni avec le switch). Le driver mini USB est disponible dans la section de téléchargement du firmware sur le site http://www.rockwellautomation.com.
Ports en liaison montante à double fonction	Les deux ports en liaison montante à double fonction disponible sur certains modèles peuvent être configurés pour les types de liaison RJ45 (cuivre) ou SFP (fibre). Une seule de ces connexions peut être active à la fois dans chacun des ports à double fonction. Si les deux ports sont connectés, le port de module SFP a la priorité. Vous pouvez configurer les ports cuivre RJ45 pour fonctionner à 10, 100 ou 1 000 Mbits/s (le débit de 1 000 Mbits/s n'est pas pris en charge sur tous les modules avec ports mixtes), en duplex intégral ou en half-duplex. Vous pouvez les configurer comme ports Ethernet fixés à 10, 100 ou 1 000 Mbits/s (Gigabit) et pouvez configurer le paramètre duplex. Vous pouvez utiliser des modules SFP Ethernet Gigabit (ou 100 Mbits/s) pour établir des connexions à fibre optique vers d'autres switchs. Ces modules émetteurs/récepteurs sont remplaçables sur site et fournissent les interfaces de liaison montante, une fois insérés dans un emplacement de module SFP. Vous utilisez des câbles à fibre optique avec des connecteurs LC pour effectuer une connexion vers un module SFP à fibre optique. Ces ports fonctionnent uniquement en duplex intégral.
Ports 10/100	Vous pouvez configurer les ports 10/100 pour fonctionner à 10 ou 100 Mbits/s, en duplex intégral ou en half-duplex. Vous pouvez également configurer ces ports pour une négociation automatique de la vitesse et du duplex conformément à la norme IEEE 802.3-2002. (La négociation automatique est le paramètre par défaut.) Lorsqu'il est configuré pour la négociation automatique, le port détecte la vitesse et le paramètre duplex du dispositif connecté. Si le dispositif connecté prend également en charge la négociation automatique, le port du switch négocie la meilleure connexion (c'est-à-dire la vitesse de ligne la plus élevée prise en charge par les deux dispositifs ainsi que la transmission en duplex intégral si le dispositif connecté prend cela en charge) et se configure en conséquence. Dans tous les cas, le dispositif attaché doit être à moins de 100 m du switch.
Ports PoE	Les ports PoE disponibles sur certains modèles peuvent être configurés pour PoE (IEEE 802.3af) ou PoE+ (IEEE 802.3at Type 2) : • Pour la configuration PoE, les ports PoE requièrent une source d'alimentation externe à 2 fils de 48 V c.c.. • Pour la configuration PoE+, les ports PoE requièrent une source d'alimentation externe à 2 fils de 54 V c.c..
Auto-MDIX	Pour la connexion du switch à des stations de travail, des serveurs et des routeurs, des câbles droits sont normalement utilisés. Toutefois, la fonctionnalité de croisement d'interface automatique en fonction du support (auto-MDIX) du switch est activée par défaut et reconfigure automatiquement les ports de manière à utiliser un type de câble soit droit, soit croisé. La fonction Auto-MDIX est activée par défaut. Lorsque la fonction auto-MDIX est activée, le switch détecte le type de câble requis (droit ou croisé) pour les connexions Ethernet en cuivre et configure les interfaces en conséquence. Vous pouvez utiliser l'interface de ligne de commande (CLI) pour désactiver la fonction auto-MDIX. Consultez l'aide en ligne pour de plus amples informations.

Fichiers de configuration

Le fichier de configuration du switch (config.txt) est en format ASCII lisible par l'utilisateur. Ce fichier de configuration est stocké dans la mémoire non volatile. Il est lu dans la mémoire vive (RAM) du switch en tant que configuration en cours d'exécution lorsque le switch est mis sous tension. Lorsque des modifications sont apportées à la configuration, les modifications prennent immédiatement effet dans la configuration en cours d'exécution. L'interface Internet de Device Manager et le profil complémentaire (AOP) pour l'application Logix Designer écrivent automatiquement les modifications vers la mémoire flash de manière à ce qu'elles soient retenues lors du cycle de mise sous tension suivant. Toutes les modifications apportées via la CLI doivent être écrites manuellement vers la mémoire flash pour être retenues lors du cycle de mise sous tension suivant.

Carte SD

Le switch est équipé d'un emplacement pour une carte Secure Digital (SD) en option, en plus de la mémoire flash intégrée. La carte SD peut être utilisée à la place de la mémoire flash embarquée pour restaurer facilement une configuration de switch en cas de défaillance ou pour dupliquer facilement des configurations lorsque vous déployez un nouveau réseau.

Si la carte SD est installée sur le switch, celui-ci démarre l'IOS et la configuration présents sur la carte SD. Si la carte SD n'est pas installée ou si les fichiers ne sont pas présents, le switch lit les paramètres d'amorçage embarqués et redémarre à partir de l'image IOS spécifiée dans la mémoire flash intégrée.

Vous devez utiliser la carte SD disponible auprès de Rockwell Automation (référence 1784-SD1) avec le switch.

ATTENTION : Rockwell Automation se réserve le droit de refuser toute assistance en cas d'utilisation d'une carte SD non fournie par Rockwell dans ce produit.

Si vous démarrez à partir de la carte SD et puis la retirez alors que le switch est en cours de fonctionnement, les conditions suivantes s'appliquent :

- L'interface Internet de Device Manager n'est plus accessible.
- Les modifications apportées à l'aide de l'interface CLI ou de l'AOP prendront effet, mais ne sont pas enregistrées lorsque le switch est redémarré.
- Si la carte SD est réinsérée dans l'emplacement, les modifications ne sont pas enregistrées sur la carte à moins que de nouvelles modifications ne soient effectuées. L'ensemble de la configuration est ensuite enregistré sur la carte.

ATTENTION : les cartes SD comportent communément un interrupteur physique de verrouillage contre l'écriture. Si cet interrupteur est engagé, le switch démarre sans problème à partir de la carte SD. Les modifications apportées à l'aide de l'interface CLI, de l'AOP ou de l'interface Internet de Device Manager prendront effet, mais ne sont pas enregistrées lorsque le switch est redémarré.

Synchronisation de la carte SD

Vous pouvez utiliser l'interface Internet de Device Manager ou l'AOP pour l'application Logix Designer pour synchroniser la carte SD pour la configuration et les mises à jour de l'IOS. Le processus de synchronisation de la configuration synchronise les fichiers config.text et vlan.dat provenant de la source choisie vers la destination choisie.

Le processus de synchronisation de l'image IOS synchronise l'image IOS de démarrage existante de la source choisie vers la destination choisie. Ce processus prend environ cinq minutes.

Si d'autres fichiers, tels que des configurations de sauvegarde, sont présents sur la carte SD, ceux-ci ne sont pas synchronisés.

ATTENTION : lors de la synchronisation, gardez à l'esprit votre source de démarrage afin de déterminer le sens de la synchronisation. Device Manager fournit cette information sous l'onglet de synchronisation de la carte SD. Vous pouvez écraser la configuration de votre choix si vous synchronisez dans la mauvaise direction.

Allocation de mémoire du switch

Le tableau suivant fournit des détails sur l'allocation de mémoire par défaut pour les switchs.

Vous pouvez utiliser des modèles SDM pour configurer les ressources système dans le switch de manière à optimiser la prise en charge de fonctionnalités spécifiques, selon la manière dont le switch est utilisé dans le réseau. Vous pouvez sélectionner un modèle afin de fournir une utilisation maximale du système pour certaines fonctions : par exemple, utilisez le modèle par défaut afin d'équilibrer les ressources et utilisez le modèle d'accès pour obtenir le maximum d'utilisation ACL. Pour affecter des ressources matérielles pour différents usages, les modèles SDM du switch gèrent les priorités des ressources système afin d'optimiser la prise en charge de certaines fonctionnalités.

Les modèles SDM suivants sont disponibles :

- Valeurs par défaut
- Routage
- IPv6 et IPv4 double

Envisagez d'utiliser le modèle de routage si vous avez activé le routage statique, ou si vous avez plus de 180 groupes IGMP ou itinéraires multidiffusion. Envisagez d'utiliser le modèle double IPv4 et IPv6 si vous utilisez IPv6.

Vous pouvez sélectionner les modèles SDM pour le protocole IP version 4 (IPv4) afin d'optimiser ces fonctionnalités.

Fonctionnalité	Allocation de mémoire		
	Valeurs par défaut	Routage	IPv6 et IPv4 double
Adresses MAC à envoi individuel	8 K	4 K	7,5 K
Groupes IGMP IPv4 + routes à multidiffusion	0,25 K	0,25 K	0,25 K
Itinéraires d'envoi individuel IPv4	0	4,25 K	0
Groupes de multidiffusion IPv6	0	0	0,375 K
Hôtes IPv4 directement connectés	0	4 K	
Adresses IPv6 directement connectées	0	0	o
Routes IPv4 indirectes	0	0,25 K	
Routes IPv6 indirectes	0	0	0
Accès de routage à base de politiques IPv4	0	0	
Accès QoS IPv4/MAC	0,375 K	0,375 K	0,375 K
Accès de sécurité IPv4/MAC	0,375 K	0,375 K	0,375 K
Accès de routage à base de politiques IPv6	0	0	0
Accès QoS IPv6	0	0	0
Accès de sécurité IPv6	0	0	0,125 K

Interface Internet de Device Manager

Vous pouvez gérer le switch à l'aide de l'interface Internet de Device Manager. L'interface Internet de Device Manager est un outil de gestion graphique de dispositif servant à configurer, à surveiller et à dépanner des switchs individuels.

L'interface Internet de Device Manager affiche des vues en temps réel des performances et de la configuration du switch. Il simplifie les tâches de configuration avec des fonctionnalités telles que les Smartports afin de configurer rapidement le switch et ses ports. Il utilise des écrans graphiques à codes de couleur, tels que la vue de la face avant, ainsi que des graphiques et des indicateurs animés afin de simplifier les tâches de surveillance. Il fournit des outils d'alertes pour vous aider à identifier et à résoudre les problèmes du réseau.

Vous pouvez afficher l'interface Internet de Device Manager de n'importe où dans votre réseau à travers un navigateur Internet tel que Microsoft Internet Explorer.

Configuration matérielle requise

Attribut	Exigence
Vitesse du processeur	1 GHz ou plus rapide (32 bits ou 64 bits)
RAM	1 Go (32 bits) ou 2 Go (64 bits)
Espace disque	16 Go (32 bits) ou 20 Go (64 bits)
Nombre de couleurs	256
Résolution	1 024 x 768
Taille de police	Petite

Configuration logicielle requise

Navigateur Internet	Version
Microsoft Internet Explorer	9.0, 10.0 ou 11.0 avec JavaScript activé
Mozilla Firefox	25 ou 26 avec JavaScript activé

L'interface Internet de Device Manager vérifie la version du navigateur au démarrage d'une session afin d'assurer que le navigateur est pris en charge.

CONSEIL Afin que l'interface Internet de Device Manager s'exécute correctement, désactivez tout bloqueur de pop-up ou réglage de proxy dans votre logiciel de navigation ainsi que tous les clients sans fil en cours d'exécution sur votre ordinateur de bureau ou votre ordinateur portable.

Environnement Studio 5000

Vous pouvez gérer le switch à l'aide de l'application Logix Designer dans l'environnement Studio 5000. L'application Logix Designer est conforme à la norme CEI 61131-3 et propose des éditeurs de logique à ralais,texte structuré, diagramme de blocs fonctionnels et graphe de fonctionnement séquentiel pour vous permettre de développer des programmes d'application.

Configuration matérielle requise

Attribut	Exigence
Vitesse du processeur	Pentium II 450 MHz (min.) Pentium III 733 MHz (ou plus) recommandé
RAM	128 Mo (min.) 256 Mo recommandés
Espace libre sur le disque dur	3 Go
Lecteurs optiques	DVD
Configuration vidéo requise	Carte graphique VGA 256 couleurs résolution 800 x 600 min (True Color 1 024 x 768 recommandé)
Résolution	résolution 800 x 600 min (True Color 1 024 x 768 recommandé)

Cisco Network Assistant

Cisco Network Assistant est une interface Internet que vous pouvez télécharger depuis le site Internet de Cisco et exécuter sur votre ordinateur. Il offre des options avancées pour la configuration et la surveillance de multiples dispositifs, y compris les switchs, les groupes de switchs, les piles de switchs, les routeurs et les points d'accès.

Suivez les étapes ci-après pour utiliser le logiciel.

1. Rendez-vous sur le site http://www.cisco.com/go/NetworkAssistant.

   Vous devez être un utilisateur enregistré, mais n'avez besoin d'aucun autre privilège d'accès.
2. Trouvez le programme d'installation Network Assistant.
3. Téléchargez le programme d'installation de Network Assistant et exécutez-le.

   Vous pouvez l'exécuter directement depuis Internet si votre navigateur vous offre ce choix.
4. Lorsque vous exécutez le programme d'installation, suivez les instructions affichées.
5. Dans le panneau final, cliquez sur Finish pour terminer l'installation de Network Assistant.
6. Consultez l'aide en ligne de Network Assistant pour de plus amples informations.

Interface de ligne de commande

Vous pouvez gérer le switch depuis l'interface de ligne de commande (CLI) en connectant votre ordinateur personnel directement au port de console du switch ou par l'intermédiaire du réseau à l'aide de Telnet.

Pour accéder à la CLI via le port de la console, suivez ces étapes.

1. Connectez-vous au port console d'une des manières suivantes :
   - Utilisez un câble adaptateur RJ45/DB-9 (non fourni avec le switch) pour connecter le switch au port série à 9 broches standard sur un ordinateur personnel.
   - Utilisez un câble mini-USB standard (non fourni avec le switch) pour connecter le switch au port mini-USB sur un ordinateur personnel.
   - Si vous utilisez le câble USB, téléchargez les drivers pour votre ordinateur Microsoft Windows sur le site http://www.rockwellautomation.com.
2. Reliez l'autre extrémité du câble au port de la console sur le switch.

   AVERTISSEMENT : le port de la console est prévu uniquement à des fins de programmation locale temporaire et n'est pas prévu pour une connexion permanente. Si vous branchez ou débranchez le câble de la console alors que ce module ou le dispositif de programmation à l'autre extrémité du câble sont alimentés, un arc électrique peut se produire, susceptible de provoquer une explosion dans des installations en environnement dangereux. Assurez-vous que l'alimentation est coupée ou que l'environnement est classé non dangereux avant de poursuivre.
3. Démarrez un programme d'émulation de terminal sur l'ordinateur personnel.
4. Configurez le logiciel d'émulation de terminal sur l'ordinateur personnel sur 9 600 bits, 8 bits de données, sans parité, 1 bit d'arrêt et sans contrôle de flux.

Notes :

Installation du switch

Consignes d'installation

ATTENTION : cet équipement est adapté uniquement à une utilisation dans les emplacements de Classe I, Division 2, groupes A, B, C, D ou non dangereux.

Au terme de son cycle de vie, cet équipement doit être mis au rebut séparément des ordures ménagères non triées.

Au moment de déterminer l'emplacement du switch, observez les consignes suivantes :

- La circulation de l'air autour du switch doit s'effectuer sans restrictions. Pour éviter tout risque de surchauffe, respectez les dégagements minimaux suivants :
  - Haut et bas : 50,8 mm (2,0 in.)
  - Côtés : 50,8 mm (2,0 in.)
  - Avant : 50,8 mm (2,0 in.)
- Pour les ports 10/100 et 10/100/1 000, la longueur du câble entre le switch et un dispositif connecté ne doit pas dépasser 100 mètres.
- La longueur de câble à fibre optique entre un switch et un dispositif connecté ne peut pas dépasser la distance indiquée à l'Annexe C.
- Pour une immunité maximale contre le bruit, des câbles blindés doivent être utilisés sur les ports de liaison montante RJ45 (IG1/1 et IG1/2) des switchs suivants :
  - 1783-BMS06TGL
  - 1783-BMS06TGA
  - 1783-BMS10CGL
  - 1783-BMS10CGA
  - 1783-BMS10CGN
  - 1783-BMS10CGP
  - 1783-BMS12T4E2CGNK
  - 1783-BMS12T4E2CGP
  - 1783-BMS12T4E2CGL
  - 1783-BMS20CGL
  - 1783-BMS20CGN
  - 1783-BMS20CGP
  - 1783-BMS20CGPK
- La température ambiante autour de l'unité ne doit pas dépasser 60 °C (140 °F).

IMPORTANT Lorsque le switch est installé dans un boîtier industriel, la température à l'intérieur du boîtier est supérieure à la température ambiante à l'extérieur du boîtier.

La température à l'intérieur ne doit pas dépasser 60 °C (140 °F), la température ambiante maximale en boîtier du switch.

- Le dégagement des faces avant et arrière doit remplir les conditions suivantes :
  - les voyants d'état en face avant doivent être facilement lisibles ;
  - l'accès aux ports est suffisant pour faciliter le câblage ;
  - les connecteurs d'alimentation en courant continu (c.c.) et le relais d'alarme de la face avant sont à portée de la connexion à l'alimentation électrique c.c..
- éloignez le câblage des sources de bruit électrique, telles que les radios, les lignes électriques et les lampes fluorescentes ;
- Reliez l'unité uniquement à une source d'alimentation c.c. de classe 2.

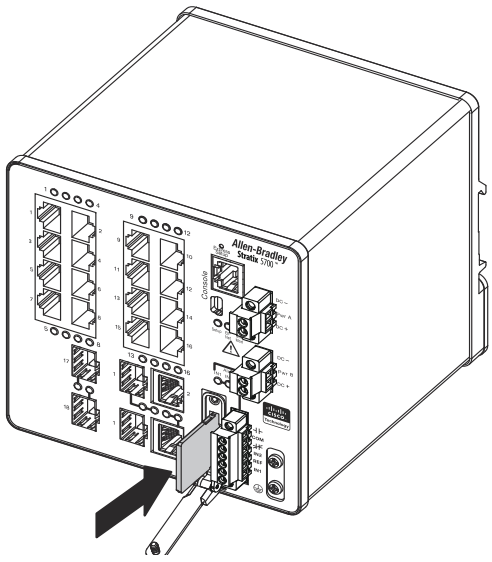
Installer ou retirer la carte SD (en option)

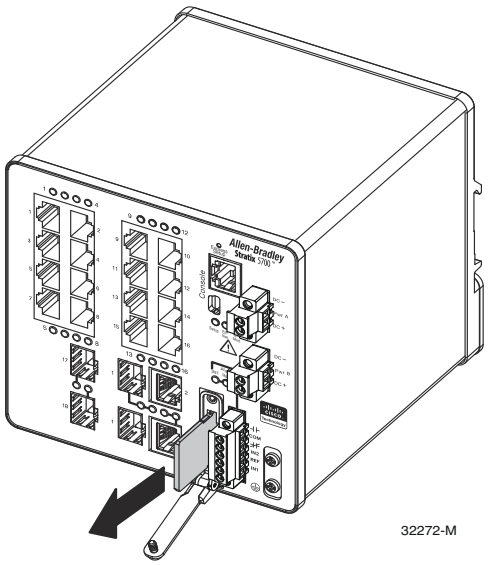
Pour installer ou remplacer la carte SD, suivez ces étapes.

1. Sur l'avant du switch, repérez la porte qui protège l'emplacement de carte SD.
2. Desserrez la vis à molette imperdable au dessus de la porte à l'aide d'un tournevis pour ouvrir la porte.
   a. Pour installer une carte, glissez-la dans l'emplacement et appuyez fermement jusqu'à ce qu'elle enclenche le mécanisme de verrouillage à ressort.

      La carte comporte un détrompeur qui vous empêche de l'introduire complètement dans le mauvais sens.
   b. Pour retirer la carte, poussez-la et laissez le mécanisme à ressort l'éjecter.
   c. Saisissez le haut de la carte et retirez-la.

      Placez-la dans un sac antistatique pour la protéger contre les décharges statiques.





3. Après l'installation de la carte, fermez la porte de protection et fixez la vis imperdable à l'aide d'un tournevis pour maintenir la porte en place.

Vérifier le fonctionnement du switch

Avant d'installer le switch dans son emplacement final, mettez-le sous tension et vérifiez qu'il démarre correctement.

Le temps requis pour le démarrage du switch est directement lié à sa configuration. Le temps de démarrage est affecté négativement entre autres par les éléments suivants :

- Mode d'apprentissage Spanning Tree
- Nombre de fichiers ou d'images dans la mémoire flash embarquée

Suivez les étapes ci-dessous pour tester le switch.

1. Mettez le switch sous tension.

   Pour mettre sous tension un switch directement connecté à une source d'alimentation c.c., localisez le disjoncteur sur le panneau qui dessert le circuit c.c. puis mettez-le en position ON.

2. Vérifier la séquence de démarrage.

   Lorsque vous mettez le switch sous tension, il commence automatiquement une rapide routine de démarrage. Le voyant d'état du système clignote en vert lors du chargement de l'image du logiciel IOS. Si la routine échoue, le voyant d'état du système passe au rouge.

   ATTENTION : les échecs de démarrage causent généralement des dégâts irrémédiables au switch. Contactez immédiatement votre représentant Rockwell Automation si votre switch ne réussit pas la séquence de démarrage.

   IMPORTANT Vous pouvez désactiver l'amorçage rapide et effectuer une autovérification au démarrage (POST) à l'aide de l'interface de ligne de commande IOS. Consultez la documentation appropriée à l'adresse http://www.Cisco.com pour de plus amples informations.

3. Après avoir exécuté ce test avec succès, effectuez ces opérations :
   a. Mettez le switch hors tension.
   b. Déconnectez les câbles.
   c. Décidez de l'endroit où vous souhaitez installer le switch.

Connecter la mise à la terre et l'alimentation c.c.

Ces sections décrivent les étapes nécessaires pour relier une terre protectrice et une alimentation c.c. au switch.

Pour les connexions d'alimentation c.c., utilisez des câbles en cuivre électroménager à paire torsadée de style 1 007 ou 1 569 -aux normes UL ou CSA, tels que le câble Belden référence 9318.

Mise à la terre du switch

ATTENTION : cet équipement doit être mis à la terre. Ne contournez jamais le conducteur de terre et n'utilisez jamais l'équipement en l'absence d'un conducteur de terre convenablement installé. Contactez l'autorité d'inspection électrique appropriée ou un électricien si vous n'êtes pas certains qu'une mise à la terre adaptée est disponible.

Cet équipement est prévu pour être relié à la terre afin de se conformer aux exigences en matière d'émissions et d'immunité. Assurez-vous que la cosse de terre fonctionnelle du switch est connectée à la terre pendant l'utilisation normale.

ATTENTION : afin de garantir que l'équipement est connecté à la terre de manière fiable, suivez les instructions de la procédure de mise à la terre et utilisez une cosse annulaire homologuée UL adaptée aux fils de calibre AWG 10 à 12, tels que la cosse Thomas & Betts référence 10RCR ou équivalente.

Utilisez un fil de calibre AWG 12 (4 mm^2) au minimum pour relier à la vis de mise à la terre externe.

La cosse de terre n'est pas fournie avec le switch. Vous pouvez utiliser l'une des options suivantes :

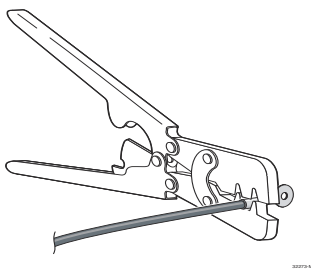
- Une borne avec cosse annulaire unique
- Deux bornes avec cosse annulaire unique

Suivez les étapes ci-dessous pour mettre le switch à la terre. Assurez-vous de suivre toutes les exigences de mise à la terre sur votre site.

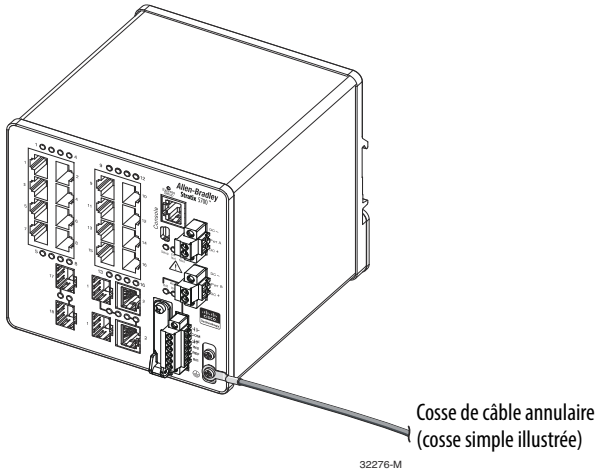
1. Utilisez un tournevis cruciforme ou un tournevis dynamométrique à cliquet muni d'une tête cruciforme pour retirer la vis de mise à la terre de la face avant du switch.

   Mettez la vis de mise à la terre de côté pour une utilisation ultérieure.
2. Suivez les consignes du fabricant pour déterminer la longueur de fil à dénuder.
3. Insérez le fil de mise à la terre dans la cosse annulaire et, à l'aide d'un outil de sertissage, sertissez la cosse sur le fil.

   Si vous utilisez deux cosses annulaires, répétez cette action sur la deuxième.



4. Faites glisser la vis de mise à la terre dans la cosse.
5. Insérez la vis de mise à la terre dans le trou de vis de mise à la terre fonctionnelle sur la face avant.



6. Utilisez un tournevis dynamométrique à cliquet pour serrer les vis de mise à la terre et les cosses annulaires sur la face avant avec un couple de 0,4 N•m

   Ne dépassez pas le couple recommandé.
7. Fixez l'autre extrémité du fil de masse à une surface en métal nu mise à la terre, telle qu'une barre de terre, un rail DIN mis à la terre, ou un châssis nu mis à la terre.

Câbler la source d'alimentation c.c.

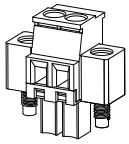
Suivez les étapes ci-dessous pour relier l'alimentation c.c. au switch.

ATTENTION : avant d'entreprendre les procédures suivantes, assurez-vous que l'alimentation est coupée sur le circuit c.c. ou que l'environnement est classé non dangereux avant de poursuivre.

- Ce produit est prévu pour être alimenté par une source d'alimentation de classe 2 marquée « Classe 2 » et dimensionnée pour 12, 24 ou 48 V c.c., 2,5 A.
- Pour se conformer à la Directive basse tension CE, cet équipement doit être alimenté à partir d'une source conforme à la très basse tension de sécurité (TBTS) ou à la très basse tension de protection (TBTP).
- Un dispositif sectionneur à deux pôles facilement accessible doit être incorporé au câblage fixe.
- Ce produit repose sur l'installation du bâtiment pour la protection contre les courts-circuits (surintensité). Assurez-vous que le dispositif de protection est évalué à un maximum de 3 A.
- L'installation de l'équipement doit être conforme aux codes électriques locaux et nationaux.
- Seul un personnel formé et qualifié doit être autorisé à effectuer l'installation, le remplacement ou l'entretien de cet équipement.

ATTENTION : pour les connexions des fils sur l'alimentation et le connecteur de relais, vous devez utiliser des câbles en cuivre électroménager à paire torsadée de style 1 007 ou 1 569 aux normes UL ou CSA, tels que le câble Belden référence 9318.

1. Localisez la prise d'alimentation.



32280-M

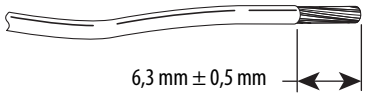
2. Identifiez les connexions c.c. positive et de retour.

   La connexion d'alimentation c.c. positive est marquée DC+ ; la connexion d'alimentation c.c. négative est la connexion adjacente marquée DC-.

3. Mesurez une longueur de fil de cuivre de 0,82 à 0,52 mm^2 (18 à 20 AWG) suffisante pour la connexion à la source d'alimentation c.c..

4. À l'aide d'un outil de dénudage pour calibre 18 AWG, dénudez chaque fil sur 6,3 mm ± 0,5 mm.

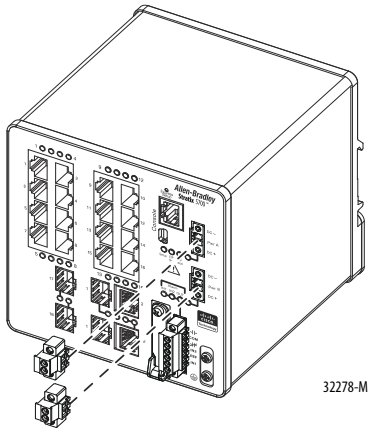
   Ne dénudez pas plus de 6,8 mm d'isolant sur le fil. Dénuder une longueur de fil supérieure à la longueur recommandée peut laisser une longueur de fil dénudé après l'installation.



31789-M

5. Desserrez les deux vis imperdables qui fixent le connecteur d'alimentation au switch et retirez le connecteur d'alimentation.

   Retirez les deux connecteurs si vous effectuez un raccordement à deux sources d'alimentation.

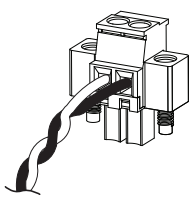


32278-M

6. Insérez la partie dénudée du fil positif dans la connexion marquée DC+ et la partie dénudée du fil de retour dans la connexion marquée DC-.

   Assurez-vous qu'aucune partie de fil dénudé n'est visible. Seuls des fils isolés peuvent dépasser du connecteur.

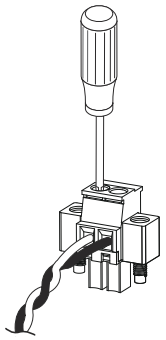
ATTENTION : une partie exposée de fil dénudé d'alimentation électrique c.c. peut conduire des niveaux dangereux d'électricité. Assurez-vous qu'aucune partie exposée du fil d'entrée d'alimentation c.c. ne dépasse du ou des connecteurs ou des borniers.



32279-M

7. Utilisez un tournevis dynamométrique à cliquet pour serrer les vis imperdables du connecteur d'alimentation (au-dessus des fils installés) avec un couple maximum de 0,23 Nm.

   Ne dépassez pas le couple recommandé.

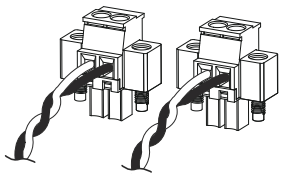


32281-M

8. Connectez l'autre extrémité du fil positif sur la borne positive de la source d'alimentation c.c. puis connectez l'autre extrémité du fil de retour à la borne de retour sur la source d'alimentation c.c.

   Lorsque vous testez le switch, un seul raccordement d'alimentation suffit. Si vous installez le switch et utilisez une seconde source d'alimentation, répétez cette procédure avec le second connecteur d'alimentation.

   La figure suivante montre le câblage d'entrée c.c. effectué sur un connecteur d'alimentation pour une source d'alimentation principale et une source d'alimentation secondaire en option.

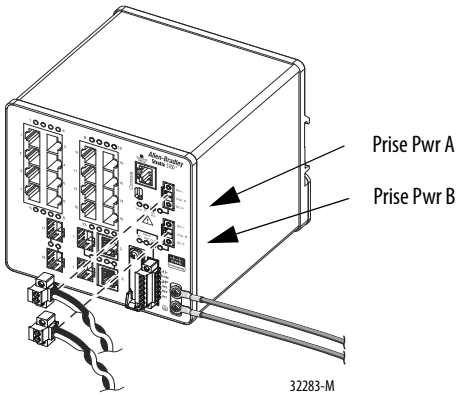


32282-M

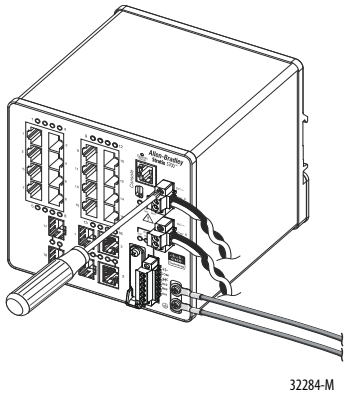
Fixer les connecteurs d'alimentation du switch

Suivez ces étapes pour fixer les connecteurs d'alimentation sur la face avant du switch.

1. Insérez un connecteur d'alimentation dans la prise Pwr A sur la face avant du switch et l'autre dans la prise Pwr B.



2. À l'aide d'un tournevis dynamométrique à cliquet, serrez les vis imperdables sur les côtés des connecteurs d'alimentation.



Lorsque vous testez le switch, une seule source d'alimentation suffit. Si vous installez le switch et utilisez une seconde source d'alimentation, répétez cette procédure pour le deuxième connecteur d'alimentation (Pwr B), qui s'installe juste en dessous du connecteur d'alimentation principal (Pwr A).

3. Lorsque vous installez le switch, fixez les fils provenant des connecteurs d'alimentation au châssis en utilisant des attaches autobloquantes.

Câbler la source d'alimentation c.c. par Ethernet (en option)

Cette procédure s'applique uniquement aux switchs avec ports PoE (Power over Ethernet).

AVERTISSEMENT : le port de la console est prévu uniquement à des fins de programmation locale temporaire et n'est pas prévu pour une connexion permanente. Si vous branchez ou débranchez le câble de la console alors que ce module ou le dispositif de programmation à l'autre extrémité du câble sont alimentés, un arc électrique peut se produire, susceptible de provoquer une explosion dans des installations en environnement dangereux. Assurez-vous que l'alimentation est coupée ou que l'environnement est classé non dangereux avant de poursuivre.

ATTENTION : pour se conformer à la Directive basse tension CE, cet équipement doit être alimenté à partir d'une source conforme à la très basse tension de sécurité (TBTS) ou à la très basse tension de protection (TBTP).

Pour se conformer aux restrictions UL, cet équipement doit être alimenté à partir d'une source de classe 2 ou à tension et courant limités.

Le switch doit être câblé et mis à la terre.

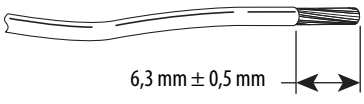
Les critères d'alimentation électrique dépendent de votre application.

Application	Alimentation par port	Consommation électrique	Produits Allen-Bradley
PoE uniquement IEEE 802.3af	44 à 57 V c.c. (48V c.c. nom.)	15,4 W (max.)	Alimentations à découpage : • 1606-XL Standard • 1606-XLE Essential • 1606-XLP Compact • 1606-XLS Performance
PoE et PoE + IEEE 802.3at Type 2	50 à 57 V c.c. (54 V c.c. nom.)	15,4 W max pour PoE 30 W max pour PoE+	

AVERTISSEMENT : avant d'entreprendre les procédures ci-dessous, assurez-vous que l'alimentation est coupée sur le circuit c.c. ou que l'environnement est classé non dangereux.

1. Mesurez une longueur de fil de cuivre de 0,82 à 0,52 mm^2 (18 à 20 AWG) suffisante pour la connexion à la source d'alimentation c.c..
2. À l'aide d'un outil de dénudage pour calibre 18 AWG, dénudez chacun des deux fils sur 6,3 mm ± 0,5 mm.

   Ne dénudez pas plus de 6,8 mm d'isolant sur le fil. Dénuder une longueur de fil supérieure à la longueur recommandée peut laisser une longueur de fil dénudé après l'installation.

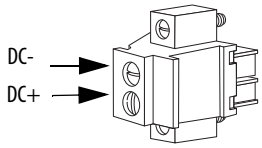


31789-M

3. Localisez la prise d'alimentation.

4. Insérez la partie dénudée du fil positif dans la connexion marquée DC+ et la partie dénudée du fil de retour dans la connexion marquée DC-.

   Assurez-vous qu'aucune partie de fil dénudé n'est visible. Seuls des fils isolés peuvent dépasser du connecteur.



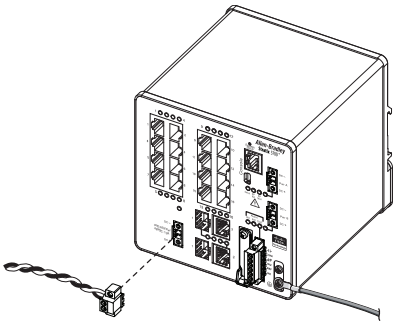
5. Utilisez un tournevis dynamométrique à cliquet pour serrer les vis imperdables du connecteur d'alimentation (au-dessus des fils installés) avec un couple maximum de 0,23 Nm.

6. Connectez l'autre extrémité du fil positif (celle connectée à DC+) à la borne positive de la source d'alimentation c.c., puis connectez l'autre extrémité du fil de retour (celle connectée à DC-) à la borne de retour de la source d'alimentation c.c..

ATTENTION : si vous utilisez différentes sources d'alimentation, ne dépassez pas la tension d'isolation spécifique.

Fixer les connecteurs d'alimentation PoE (en option)

1. Insérez le connecteur d'alimentation dans le bornier d'entrée c.c. sur la face avant du switch.
2. À l'aide d'un tournevis, serrez les vis imperdables sur les côtés du connecteur d'alimentation.



ATTENTION : l'exposition à certains produits chimiques peut dégrader les propriétés d'étanchéité des matières utilisées dans le relais. Contrôlez périodiquement le relais et surveillez toute dégradation.

Installation du switch

Cette section décrit comment installer le switch.

ATTENTION : cet équipement est fourni en tant qu'équipement de type « ouvert ». Il doit être installé à l'intérieur d'un boîtier fournissant une protection adaptée aux conditions d'utilisation ambiantes et suffisante pour éviter toute blessure corporelle pouvant résulter d'un contact direct avec des composants sous tension. L'accès à l'intérieur du boîtier ne doit être possible qu'à l'aide d'un outil.

Le boîtier doit répondre au minimum aux normes IP 54 ou NEMA type 4.

ATTENTION : pour empêcher tout risque de surchauffe, assurez-vous que les dégagements minimaux suivants sont respectés :

- Haut et bas : 50,8 mm (2,0 in.)
- Côté exposé (non connecté au module) : 50,8 mm (2,0 in.)
- Avant : 50,8 mm (2,0 in.)

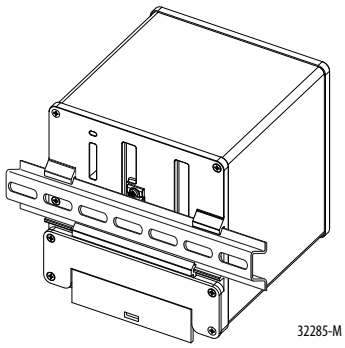
Installation du switch sur un rail DIN

Le switch dispose sur sa face arrière d'un loquet à ressort pour le montage sur un rail DIN.

ATTENTION : lorsque vous utilisez un montage sur rail DIN, une mise à la terre supplémentaire du châssis s'effectue par l'intermédiaire du rail DIN. -Utilisez un rail DIN en acier zingué chromaté jaune pour garantir une bonne mise à la terre. L'utilisation de rail DIN en d'autres matières (par exemple, en aluminium ou en plastique) pouvant se corroder et s'oxyder ou présenter une mauvaise conduction, peut se traduire par une mise à la terre incorrecte ou intermittente. Fixez le rail DIN à la surface de montage environ tous les 200 mm à l'aide d'équerres de blocage placées judicieusement et d'une plaque de boulonnage tout le long du rail DIN.

Pour fixer le switch sur un rail DIN, suivez les étapes ci-dessous.

1. Positionnez la face arrière du switch directement en face du rail DIN, en vous assurant que le rail DIN s'adapte à l'espace entre les deux crochets près du haut du switch et le loquet à ressort près du bas.
2. Tout en maintenant le bas du switch à distance du rail DIN, placez les deux crochets à l'arrière du switch sur le dessus du rail DIN.

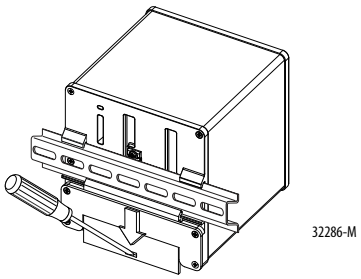


3. Poussez le switch vers le rail DIN pour que le loquet à ressort au bas de la face arrière du switch se mette en place.

Retrait du switch du rail DIN

Suivez ces étapes pour retirer le switch d'un rail DIN ou d'un châssis :

1. Coupez l'alimentation du switch et déconnectez tous les câbles et connecteurs de la face avant du switch.
2. Insérez un outil tel qu'un tournevis plat dans le logement en bas du loquet à ressort et utilisez-le pour dégager le loquet du rail DIN.



3. Retirez le switch du rail DIN.

Installation d'un module SFP (facultatif)

Sur les switchs qui prennent en charge la communication sur câble à fibre optique, des modules SFP sont insérés dans emplacements de module SFP en face avant du switch. Ces modules remplaçables sur site fournissent les interfaces optiques en liaison montante, transmission (TX) et réception (RX).

Vous pouvez utiliser n'importe quelle combinaison de modules SFP robustes. Chaque module SFP doit être du même type que le module SFP à l'autre extrémité du câble. Le câble ne doit pas dépasser la longueur stipulée pour des communications fiables.

Lorsque vous utilisez des modules SFP du commerce tels que les modules CWDM et 1000BX-U/N, réduisez la température de fonctionnement maximale de 15 °C. La température minimale de fonctionnement est de 0 °C.

Pour des instructions détaillées sur l'installation, le retrait et le câblage du module SFP, consultez la documentation de votre module SFP.

ATTENTION : nous vous recommandons fortement de ne pas installer ou retirer le module SFP tant que les câbles à fibre optique y sont fixés en raison de dommages potentiels aux câbles, au connecteur du câble ou aux interfaces optiques dans le module SFP. Débranchez tous les câbles avant de retirer ou d'installer un module SFP.

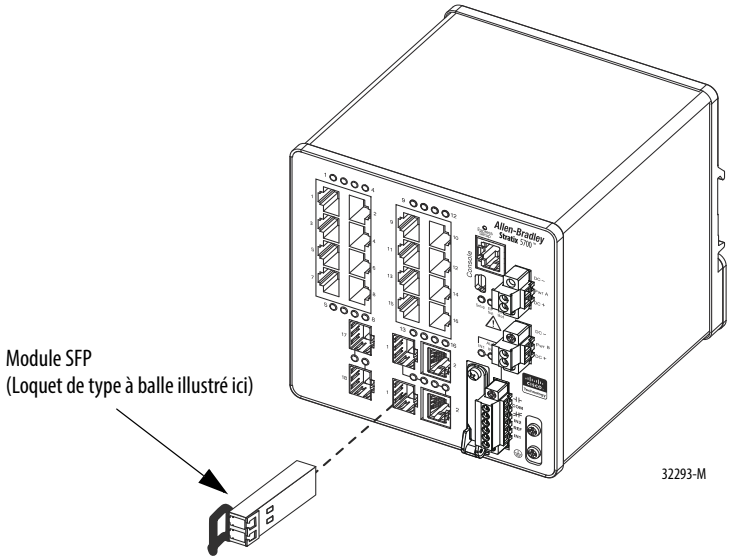
IMPORTANT Le fait d'installer et retirer un module SFP peut réduire sa durée de vie utile. Évitez de retirer et d'insérer des modules SFP plus souvent qu'il n'est absolument nécessaire.

Pour insérer un module SFP dans l'emplacement pour module SFP, suivez ces étapes.

1. Fixez un bracelet antistatique préventif à votre poignet et à une surface en métal nu mise à la terre.
2. Agrippez les deux côtés du module SFP et alignez le module sur le côté en face de l'ouverture de l'emplacement.

> **ATTENTION :** arrêtez immédiatement si le module SFP ne peut pas être entièrement inséré. Ne forcez pas le module à entrer dans le logement. Faites tourner le module SFP de 180° et essayez à nouveau.

3. Insérez le module SFP dans l'emplacement, comme illustré dans la figure suivante, jusqu'à ce que vous sentiez le connecteur sur le module s'enclencher à l'arrière de l'emplacement.



4. Retirez les bouchons antipoussière des ports optiques du module SFP, puis rangez-les pour une utilisation ultérieure.

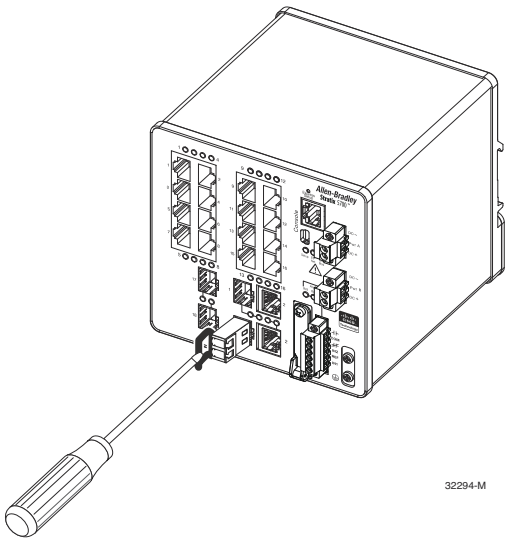
> **IMPORTANT** Ne retirez pas les bouchons antipoussière du port du module SFP ou les bouchons de caoutchouc du câble à fibre optique à moins d'être prêt à raccorder le câble.
>
> Les capuchons et bouchons protègent les ports et les câbles du module SFP de la contamination et de la lumière ambiante.

Retrait de modules SFP des emplacements pour module SFP

Pour retirer un module SFP d'une prise de module, suivez les étapes ci-dessous.

1. Fixez un bracelet antistatique préventif à votre poignet et à une surface en métal nu mise à la terre.
2. Débranchez le connecteur de fibre LC du module SFP.
3. Insérez un bouchon antipoussière dans les ports optiques du module SFP afin de maintenir la propreté des interfaces optiques.
4. Déverrouillez et retirez le module SFP.

   Si le module possède un loquet de type fermoir à balle, faites basculer la balle dans votre direction et tirez-la doucement pour éjecter le module. Si le loquet à fermoir à balle est obstrué et si vous ne pouvez pas utiliser votre index pour l'ouvrir, utilisez un petit tournevis à lame plate ou autre instrument long et étroit pour ouvrir le loquet à fermoir à balle.



5. Saisissez le module SFP entre votre pouce et votre index puis retirez-le soigneusement du logement de module.
6. Placez le module SFP retiré dans un sac antistatique ou tout autre environnement protecteur.

Câblage les alarmes externes

Le switch possède deux circuits d'entrée d'alarme et une sortie de relais d'alarme forme C (unipolaire, bidirectionnel) pour des alarmes externes. Les circuits d'entrée de relais d'alarme sont conçus pour détecter si l'entrée d'alarme est ouverte ou fermée par rapport à la broche de référence d'entrée d'alarme. Le circuit de sortie du relais d'alarme dispose d'un seul relais de forme C, avec un contact normalement ouvert (N.O.) et un contact normalement fermé (N.F.). Vous pouvez configurer le relais de sortie d'alarme comme étant normalement sous tension ou normalement hors tension à l'aide de l'interface de ligne de commande.

Reportez-vous à la section Annexe C pour un exemple de câblage d'alarme.

Les signaux d'alarme sont connectés au switch par l'intermédiaire du connecteur de relais d'alarme à 6 voies. Trois connexions sont dédiées aux deux circuits d'entrée d'alarme :

- Entrée d'alarme 1 (IN1)
- Entrée d'alarme 2 (IN2)
- Terre de référence isolée

Une entrée d'alarme ainsi que la connexion de câblage de terre de référence sont nécessaires pour compléter un seul circuit d'entrée d'alarme. Vous devez fournir un contact N.O. ou un contact N.F. pour compléter le circuit d'alarme entre la terre de référence et IN1 ou IN2.

ATTENTION : n'appliquez aucune source de tension externe aux entrées d'alarme IN1 ou IN2. Limitez le câblage de sortie d'alarme à 48 V c.c., 0,5 A.

Les trois connexions restantes, pour le circuit de sortie d'alarme forme C, sont comme suit :

- Sortie N.O.
- Sortie N.F.
- Commun

Une sortie d'alarme ainsi que la connexion de câblage du commun sont nécessaires pour réaliser un circuit de sortie d'alarme unique. Le relais de sortie d'alarme forme C fournit un contact sec N.O. et un contact sec N.F.

ATTENTION : pour les raccordements de fils sur l'alimentation et le connecteur de relais, vous devez utiliser des câbles en cuivre électroménager à paire torsadée de style 1007 ou 1569 aux normes UL ou CSA, tels que le câble Belden référence 9318.

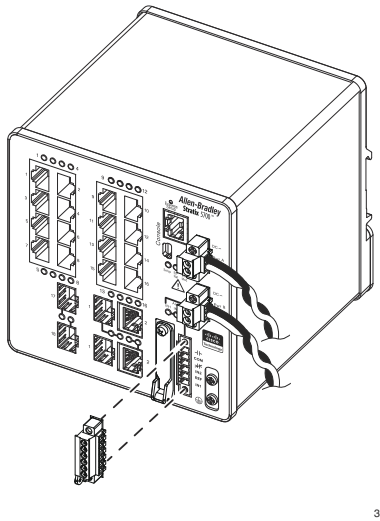
Les étiquettes pour le connecteur de relais d'alarme sont sur le panneau du switch.

Tableau 1 - Étiquettes de connecteur de relais d'alarme

Étiquette	Connexion
NO	Branchement sortie d'alarme, normalement ouvert (N.O.)
COM	Branchement commun sortie d'alarme
NC	Branchement sortie d'alarme, normalement fermé (N.F.)
IN2	Entrée d'alarme 2
REF	Branchement terre de référence d'entrée d'alarme
IN1	Entrée d'alarme 1

Suivez les étapes ci-dessous pour relier le switch à un dispositif d'alarme externe.

1. Desserrez les vis imperdables qui maintiennent le connecteur du relais d'alarme sur le switch et retirez le connecteur du châssis.



2. Mesurez deux brins de fil à paire torsadée (18 à 20 AWG) assez long pour pouvoir se connecter sur le dispositif d'alarme externe.

   Choisissez entre la mise en place d'un circuit d'entrée ou de sortie d'alarme externe.

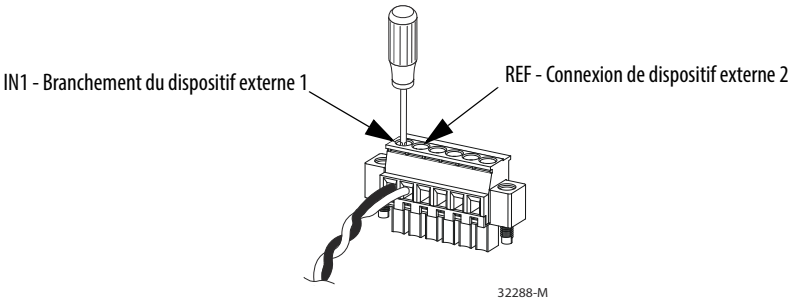
3. Utilisez une pince à dénuder pour dégager la gaine des deux extrémités de chaque fil sur 6,3 mm ± 0,5 mm.

   Ne dénudez pas plus de 6,8 mm d'isolant sur les fils. Dénuder une longueur de fil supérieure à la longueur recommandée peut laisser exposés des fils du connecteur du relais d'alarme après l'installation.

4. Insérez les fils exposés pour le dispositif d'alarme externe selon une configuration de circuit d'entrée ou de sortie d'alarme. Reportez-vous au Tableau 1 à la page 44.

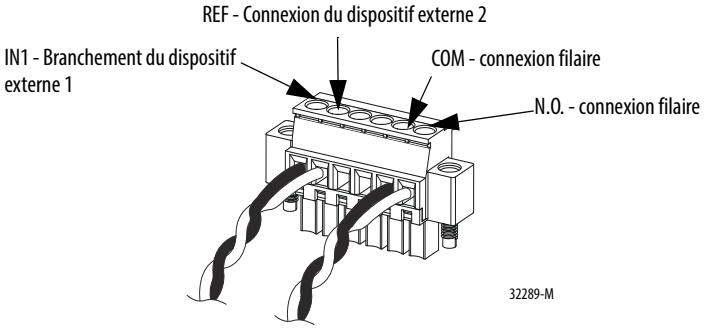
5. Utilisez un tournevis dynamométrique à cliquet pour serrer la vis imperdable du connecteur de relais d'alarme (au-dessus des fils installés) avec un couple de 0,23 Nm.

   Ne dépassez pas le couple recommandé.



6. Répétez la procédure ci-dessus pour insérer les fils d'entrée et de sortie d'un dispositif d'alarme externe supplémentaire dans le connecteur du relais d'alarme.

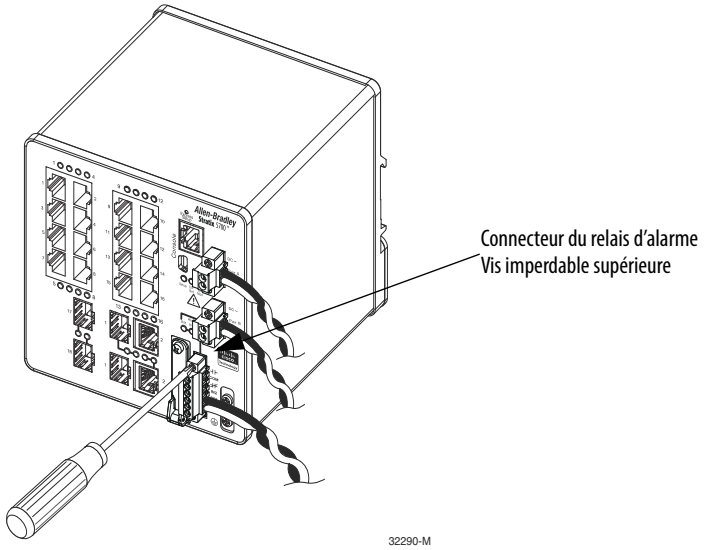
   La figure suivante illustre le câblage terminé pour deux dispositifs d'alarme externe. Le premier circuit de dispositif d'alarme est câblé comme un circuit d'entrée de relais d'alarme : les connexions IN1 et REF complètent le circuit. Le deuxième circuit de dispositif d'alarme est câblé comme un circuit de sortie du relais d'alarme en utilisant le côté normalement ouvert des contacts de relais de forme C. Les connexions N.O. et COM complètent le circuit.



Fixation du connecteur de relais d'alarme au switch

Pour fixer le connecteur du relais d'alarme sur la face avant du switch, suivez les étapes ci-dessous.

1. Insérez le connecteur du relais d'alarme dans la prise sur la face avant du switch.
2. À l'aide d'un tournevis dynamométrique à cliquet, serrez les vis imperdables sur les côtés du connecteur du relais d'alarme.



Connexion des ports de destination

Suivez les procédures ci-dessous pour effectuer les connexions vers les ports de destination.

Connexion aux ports 10/100 et 10/100/1 000

Les ports 10/100/1 000 du switch se configurent automatiquement d'eux-mêmes de manière à fonctionner à la vitesse des dispositifs connectés. Si les ports attachés ne supportent pas la négociation automatique, vous pouvez définir explicitement les paramètres de vitesse et de duplex. Connecter des dispositifs incapables de négociation automatique ou dont les paramètres de vitesse et de duplex sont définis manuellement peut réduire les performances ou aboutir à une absence de liaison.

La fonction Auto-MDIX est activée par défaut. À moins que cette fonctionnalité soit désactivée, vous pouvez utiliser des câbles aussi bien droits que croisés pour la liaison avec d'autres dispositifs sur le réseau.

Pour augmenter au maximum les performances, choisissez l'une des méthodes suivantes pour la configuration de la connexion des ports Ethernet :

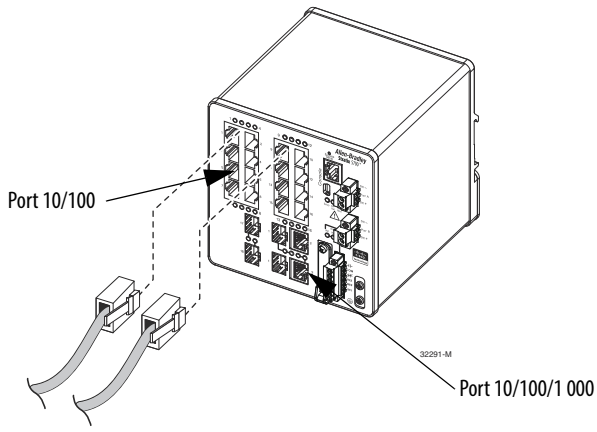
- Laissez les ports négocier automatiquement aussi bien la vitesse que le duplex
- Configurez les paramètres de vitesse et de duplex du port aux deux extrémités de la connexion

Connexion aux ports 10BASE-T, 100BASE-TX ou 1000BASE-T

Suivez les étapes ci-dessous pour la connexion aux ports 10BASE-T, 100BASE-TX ou 1000BASE-T

ATTENTION : pour empêcher les dégâts causés par les décharges électrostatiques (ESD), suivez les procédures de manipulation des circuits imprimés et des composants.

1. Choisissez l'une des options suivantes pour connecter un dispositif :
   - Lors de la connexion à des postes de travail, des serveurs et des routeurs, reliez un câble droit à un connecteur RJ45 sur la face avant.
   - Lors de la connexion à des dispositifs compatibles 1000BASE-T, utilisez un câble à quatre paires torsadées de catégorie 5e ou plus élevé.



2. Reliez l'autre extrémité du câble à un connecteur RJ45 sur l'autre dispositif.

   Le voyant d'état du port s'allume lorsque le switch et le dispositif connecté ont établi un lien.

   Le voyant d'état du port est orange lorsque le protocole STP (Spanning Tree Technology) découvre la topologie et recherche des boucles. Cela peut prendre jusqu'à 30 secondes, puis le voyant d'état du port passe au vert.

   Les conditions suivantes peuvent empêcher le voyant d'état du port de s'activer :

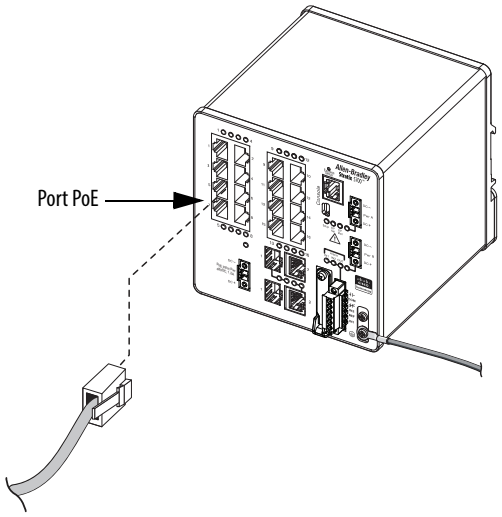
   - Le dispositif à l'autre extrémité n'est pas activé.
   - Un problème existe sur le câble ou sur l'adaptateur installé sur le dispositif attaché.

3. Reconfigurez et redémarrez le dispositif connecté si nécessaire.
4. Répétez cette procédure pour connecter chaque dispositif.

Connexion sur les ports PoE

Les switchs équipés de ports PoE requièrent une alimentation électrique séparée. Pour les besoins d'alimentation en fonction de votre application, reportez-vous à la page 37.

1. Insérez un câble direct à quatre paires torsadées de catégorie 5e ou supérieure équipé d'un connecteur RJ45 dans le port PoE.



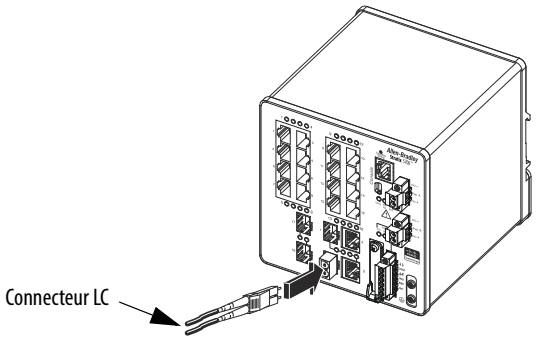
2. Insérez l'autre extrémité du câble dans un connecteur RJ45 sur l'autre dispositif à alimentation PoE.

Connexion aux modules SFP

Suivez les étapes ci-dessous pour connecter un câble à fibre optique à un module SFP.

ATTENTION : ne retirez les bouchons en caoutchouc du port du module SFP ou les capuchons de caoutchouc du câble de fibre optique que lorsque vous êtes prêt à brancher le câble. Les capuchons et bouchons protègent les ports et les câbles du module SFP de la contamination et de la lumière ambiante.

1. Retirez les bouchons en caoutchouc du port du module et du câble à fibre optique puis rangez-les pour une utilisation ultérieure.
2. Insérez une extrémité du câble à fibre optique dans le port du module SFP.



3. Insérez l'autre extrémité du câble dans une prise pour fibre optique sur un dispositif cible.
4. Observez le voyant d'état du port :
   - Le voyant d'état devient orange lorsque le SFP détecte la topologie du réseau et recherche les boucles. Cela peut prendre jusqu'à 30 secondes, puis le voyant d'état du port passe au vert.
   - Le voyant d'état du port passe au vert lorsque le switch et le dispositif cible ont établi un lien.
   - Le voyant d'état s'éteint si le dispositif cible n'est pas activé ou s'il existe un problème sur le câble ou sur l'adaptateur installé sur le dispositif cible.

   Si nécessaire, reconfigurez et redémarrez le switch ou le dispositif cible.

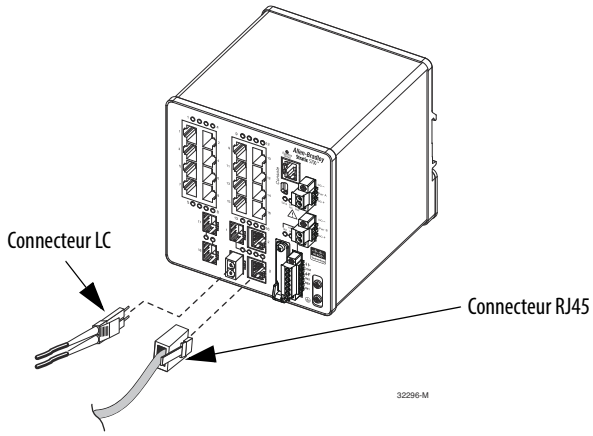
Connexion à un port à double usage

Un port à double usage est un port unique muni de deux interfaces, une destinée à un câble RJ45 et une autre pour un module SFP homologué. Une seule interface peut être active à la fois. Si les deux interfaces sont connectées, le module SFP a priorité.

ATTENTION : ne retirez les bouchons en caoutchouc du port du module SFP ou les capuchons de caoutchouc du câble de fibre optique que lorsque vous êtes prêt à brancher le câble. Les capuchons et bouchons protègent les ports et les câbles du module SFP de la contamination et de la lumière ambiante.

Suivez les étapes ci-dessous pour effectuer une connexion vers un port à double usage.

1. Reliez un connecteur RJ45 au port 10/100/1 000 ou installez un module SFP dans l'emplacement pour module SFP puis connectez un câble au port du module SFP.



2. Reliez l'autre extrémité du câble à l'autre dispositif.

   Par défaut, le switch détecte si un connecteur RJ45 ou un module SFP est connecté à un port double usage et configure automatiquement le port en conséquence. Vous pouvez modifier ce réglage et configurer le port de manière à reconnaître uniquement un connecteur RJ45 ou un module SFP l'aide de la commande de configuration d'interface de type de média. Pour de plus amples informations, reportez-vous à la documentation appropriée sur le site http://www.Cisco.com.

Configuration initiale du switch avec Express Setup

Lorsque vous configurez le switch pour la première fois, utilisez Express Setup pour saisir l'adresse IP initiale. Cela permet l'utilisation du switch comme un switch administré. Vous pouvez ensuite accéder au switch par le biais de l'adresse IP pour toute configuration supplémentaire.

IMPORTANT N'exécutez pas Express Setup avec une carte SD insérée dans le switch.

Vous avez besoin de l'équipement suivant pour configurer le switch :

- Un ordinateur personnel équipé du système d'exploitation Windows 2000, Windows XP, Windows 2003 ou Windows Vista
- Un navigateur Internet pris en charge (Internet Explorer 9.0, 10.0 et 11.0 ou Firefox 25, 26) avec JavaScript activé
- Un câble Ethernet direct ou croisé de catégorie 5, pour connecter votre ordinateur personnel au switch

Procédez comme suit pour configurer votre ordinateur :

- Désactivez toute interface sans fil fonctionnant sur votre ordinateur personnel.
- Désactivez les autres réseaux dans votre système.
- Configurez votre ordinateur afin de déterminer automatiquement son adresse IP (DHCP) plutôt qu'une configuration statique.
- Désactivez tous les serveurs DNS statiques.
- Désactivez les paramètres de proxy du navigateur.

Les réglages du navigateur figurent généralement dans Outils > Options Internet > Connexions > Réglages LAN.

Suivez les étapes ci-dessous pour exécuter Express Setup.

1. Assurez-vous qu'au moins un port Ethernet est disponible sur le switch pour Express Setup.

   IMPORTANT N'utilisez pas le port de la console pour Express Setup.

   Pendant Express Setup, le switch agit comme un serveur DHCP. Si votre ordinateur possède une adresse IP statique, modifiez les paramètres de votre ordinateur personnel avant de commencer à utiliser temporairement DHCP.

2. Mettez le switch sous tension.

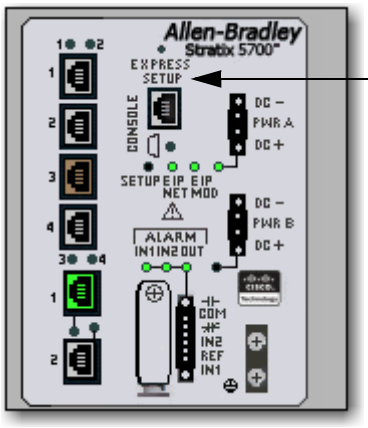
   Lorsque le switch est sous tension, il commence sa séquence de démarrage. La séquence de démarrage prend environ 60 secondes.

3. Assurez-vous que la séquence de démarrage s'est terminée en vérifiant que les voyants d'état EIP Mod et Setup clignotent en vert.

   Si le switch ne réussit pas la séquence de démarrage, le voyant d'état EIP Mod devient rouge.

4. Appuyez et relâchez le bouton Express Setup. Attendez quelques secondes jusqu'à ce que le voyant d'état sur un des ports non connectés du switch clignote en vert.

   Ce bouton est en retrait de 16 mm derrière la face avant. Utilisez un petit outil tel qu'un trombone pour atteindre le bouton.



5. Branchez un câble Ethernet de catégorie 5 (non fourni) entre le port clignotant du switch et le port Ethernet sur votre ordinateur personnel.

   CONSEIL Si vous attendez trop longtemps pour raccorder le câble, le voyant d'état Setup (configuration) s'éteint.

   Les voyants d'état de port sur votre ordinateur personnel et sur le switch clignotent pendant que le switch configure automatiquement la connexion.

6. Tandis que le voyant d'état Setup clignote en vert, démarrez une session de navigateur Internet sur l'ordinateur personnel et accédez à http://169.254.0.1.

   Si vous avez une page d'accueil configurée, la configuration de switch se charge au lieu de votre page d'accueil normale.

   Le switch vous demande le nom d'utilisateur et le mot de passe par défaut.

7. Entrez le mot de passe par défaut du switch : **switch**.

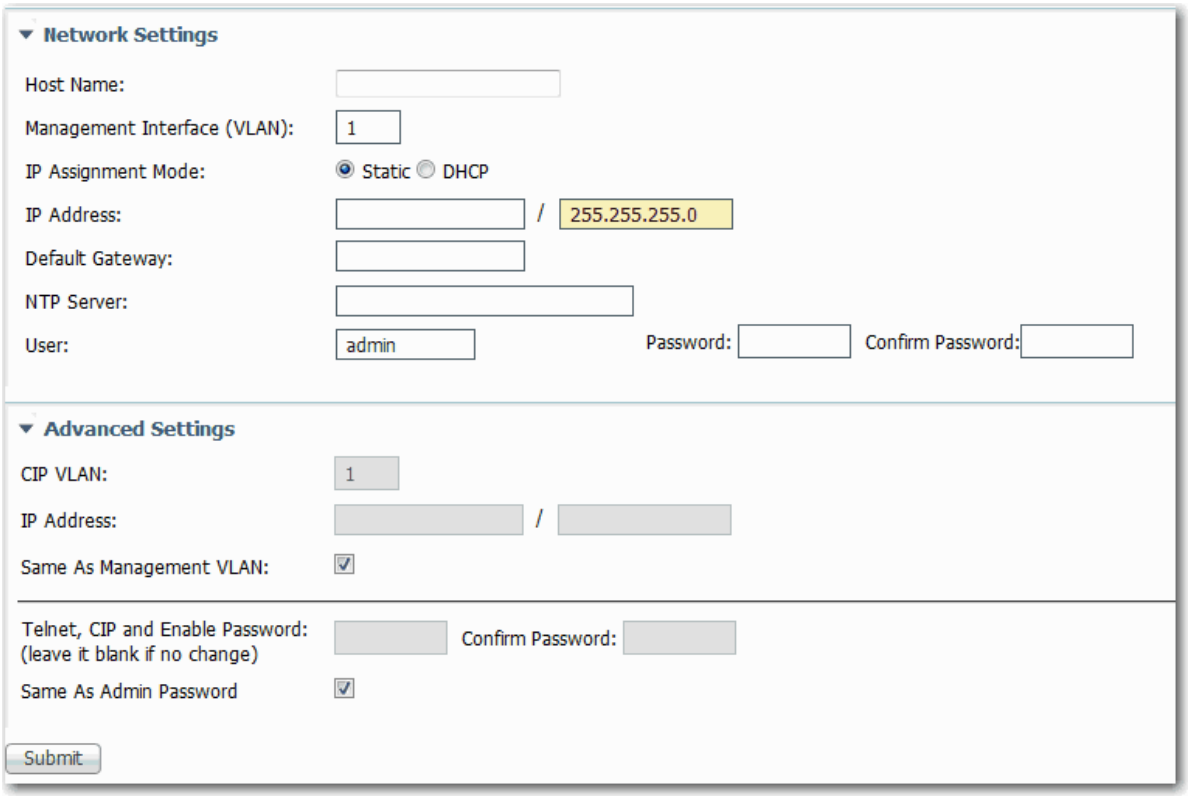
   Le nom d'utilisateur par défaut est **admin**.

   IMPORTANT Dans certains scénarios, le switch exige que vous entriez le mot de passe plusieurs fois avant de l'accepter.

8. Si la fenêtre Express Setup n'apparaît pas, procédez comme suit :
   - Saisissez l'URL d'un site Internet bien connu dans votre navigateur pour vérifier que ce dernier fonctionne correctement. Votre navigateur est automatiquement redirigé vers la page Internet Express Setup.
   - Vérifiez que les paramètres de proxy ou les bloqueurs de pop-up sont désactivés sur votre navigateur.
   - Vérifiez que toutes les interfaces sans fil sont désactivées sur votre ordinateur personnel.

9. Renseignez les champs.

   Pour afficher les champs pour le protocole industriel commun (CIP), vous devez cliquer sur Advanced Settings (paramètres évolués).



Champ	Description
	Paramètres réseau
Host Name (nom d'hôte)	Le nom du dispositif.
Management Interface (interface de gestion – VLAN ID)	Le nom et l'ID du VLAN de gestion à travers lequel le switch est administré. Choisissez un VLAN existant pour être le VLAN de gestion. L'ID par défaut est 1. Le nom par défaut du VLAN de gestion est « default ». Le nombre peut être entre 1 et 1001. Assurez-vous que le switch et la station de gestion de votre réseau sont dans le même VLAN. Dans le cas contraire, vous perdez la connectivité de gestion du switch. Le VLAN de gestion est le domaine de diffusion générale à travers lequel le trafic de gestion est envoyé entre des utilisateurs ou périphériques spécifiques. Il fournit le contrôle de diffusion générale et la sécurité pour le trafic de gestion qui doivent être limités à un groupe spécifique d'utilisateurs, tels que les administrateurs de votre réseau. Il fournit également un accès administratif sécurisé à tous les périphériques du réseau, et ce, en permanence.
IP Assignment Mode (mode d'affectation IP)	Le mode IP Assignment détermine si les informations IP du switch sont affectées manuellement (statiques) ou automatiquement par un serveur DHCP (Dynamic Host Configuration Protocol). La valeur par défaut est Static. Nous vous recommandons d'utiliser Static et d'attribuer manuellement l'adresse IP du switch. Vous pouvez ensuite utiliser la même adresse IP chaque fois que vous souhaitez accéder à l'interface Internet de Device Manager. Si vous cliquez sur DHCP, le serveur DHCP affecte automatiquement une adresse IP, un masque de sous-réseau et une passerelle par défaut au switch. Tant que le switch n'est pas redémarré, il continue à utiliser les informations IP affectées et vous êtes en mesure d'utiliser la même adresse IP pour accéder à l'interface Internet de Device Manager. Si vous affectez manuellement l'adresse IP du switch et que votre réseau utilise un serveur DHCP, assurez-vous que l'adresse IP que vous donnez au switch ne se trouve pas dans la plage d'adresses que le serveur DHCP affecte automatiquement à d'autres périphériques. Cela empêche les conflits d'adresse IP entre le switch et un autre périphérique.
IP Address (adresse IP)	L'adresse IP et le masque de sous-réseau associé sont des identificateurs uniques pour le switch dans un réseau : • L'adresse IP est une adresse numérique de 32 bits écrite sous forme de quatre nombres séparés par des points. Chaque nombre peut être compris entre 0 et 255. • Le masque de sous-réseau est l'adresse réseau qui identifie le sous-réseau auquel appartient le switch. Les sous-réseaux sont utilisés pour segmenter les périphériques d'un réseau en groupes plus petits. La valeur par défaut est 255.255.255.0. Ce champ est activé uniquement si le mode IP Assignment est Static. Assurez-vous que l'adresse IP que vous affectez au switch n'est pas utilisée par un autre périphérique dans votre réseau. L'adresse IP et la passerelle par défaut ne peuvent pas être les mêmes.
Default Gateway (passerelle par défaut – facultative)	L'adresse IP pour la passerelle par défaut. Une passerelle est un routeur ou un périphérique réseau dédié qui permet au switch de communiquer avec les périphériques dans d'autres réseaux ou sous-réseaux. L'adresse IP de passerelle par défaut doit faire partie du même sous-réseau que l'adresse IP du switch. L'adresse IP du switch et l'adresse IP de la passerelle par défaut ne peuvent pas être les mêmes. Si tous vos périphériques sont dans le même réseau et qu'une passerelle par défaut n'est pas utilisée, vous n'avez pas besoin d'entrer une adresse IP dans ce champ. Ce champ est activé uniquement si le mode IP Assignment est Static. Vous devez spécifier une passerelle par défaut si votre station de gestion de réseau et le switch se trouvent dans des réseaux ou sous-réseaux différents. Dans le cas contraire, le switch et la station de gestion de votre réseau ne peuvent pas communiquer entre eux.
NTP Server (serveur NTP)	L'adresse IP du serveur NTP (Network Time Protocol). NTP est un protocole réseau pour la synchronisation d'horloge entre les systèmes d'ordinateur sur des réseaux de données à commutation de paquets et à latence variable.
User (utilisateur)	Saisissez le nom de l'utilisateur.
Password, Confirm Password (mot de passe, confirmation de mot de passe)	Le mot de passe du switch peut comporter jusqu'à 63 caractères alphanumériques, peut commencer par un nombre, est sensible à la casse et peut incorporer des espaces. Le mot de passe ne peut pas être un chiffre unique, il ne peut pas contenir un point d'interrogation ou une tabulation et ne commence ni ne finit par un espace. La valeur par défaut est **switch**. Pour terminer la configuration initiale, vous devez modifier le mot de passe par défaut, **switch**. Ce mot de passe est également utilisé pour la sécurité du protocole de contrôle industriel (CIP). Nous vous recommandons d'attribuer un mot de passe au switch pour sécuriser l'accès au gestionnaire de dispositif.
	Paramètres évolués
CIP VLAN	Le VLAN sur lequel le protocole CIP (Common Industrial Protocol) est activé. Le CIP VLAN peut être le même que le VLAN de gestion, ou vous pouvez isoler le trafic CIP sur un autre VLAN déjà configuré sur ce dispositif.
IP Address (adresse IP)	L'adresse IP et le masque de sous-réseau pour le CIP VLAN si le CIP VLAN est différent du VLAN de gestion. Le format est une adresse numérique de 32 bits écrite sous forme de quatre nombres séparés par des points. Chaque nombre peut être compris entre 0 et 255. Assurez-vous que l'adresse IP que vous affectez à ce périphérique n'est pas utilisée par un autre périphérique sur votre réseau.
Same As Management VLAN (identique au VLAN de gestion)	Indique si les paramètres pour le CIP VLAN sont les mêmes que pour le VLAN de gestion.
Telnet, CIP et Enable Password (facultatif), Confirm Password	Le mot de passe utilisé pour la sécurité Telnet et CIP.
Same As Admin Password (identique au mot de passe Admin)	Définit que le mot de passe utilisé pour la sécurité Telnet et CIP est identique au mot de passe utilisateur indiqué pour les paramètres réseau.

10. Cliquez sur Submit (soumettre).

    Le switch initialise sa configuration pour les applications industrielles typiques EtherNet/IP. Le switch vous redirige ensuite vers la page d'ouverture de session pour l'interface Internet de Device Manager. Vous pouvez soit continuer à utiliser l'interface Internet de Device Manager pour effectuer des configurations supplémentaires, soit quitter l'application.

11. Mettez hors tension l'alimentation c.c., débranchez tous les câbles du switch et installez le switch sur votre réseau.

12. Après avoir terminé Express Setup, actualisez l'adresse IP de l'ordinateur personnel :
    - Pour une adresse IP dynamique, débranchez l'ordinateur personnel du switch et reconnectez l'ordinateur au réseau. Le serveur DHCP du réseau attribue une nouvelle adresse IP à l'ordinateur personnel.
    - Pour une adresse IP statique, modifiez l'adresse IP pour qu'elle corresponde à celle configurée précédemment.

Notes :

Fonctionnalités logicielles du switch

Numérotation des ports

L'ID du port comprend le type de port (Gigabit Ethernet pour les ports Gigabit et Fast Ethernet pour les ports 10/100 Mbits/s), le numéro d'unité (toujours 1) et le numéro du port (1-2 pour les ports Gigabit, 1-18 pour les autres en fonction des références). Les abréviations d'Ethernet Gigabit et de Fast Ethernet sont respectivement Gi et Fa.

Le tableau ci-dessous présente la numérotation des ports du switch.

Tableau 2 - Numérotation des ports

Référence	Description	Numérotation des ports sur les étiquettes du switch	Numérotation des ports dans le fichier config.text
1783-BMS06SL	switch administré à 6 ports (4 ports Ethernet, 2 emplacements SFP), firmware version légère	1 2 3 4 5 6	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6
1783-BMS06SA	switch administré à 6 ports (4 ports Ethernet, 2 emplacements SFP), firmware complet	1 2 3 4 5 6	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6
1783-BMS06TL	switch administré à 6 ports (6 ports Ethernet), firmware version légère	1 2 3 4 5 6	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6
1783-BMS06TA	switch administré à 6 ports (6 ports Ethernet), firmware complet	1 2 3 4 5 6	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6
1783-BMS06SGL	switch administré à 6 ports (4 ports Ethernet, 2 emplacements SFP), firmware version légère	1 2 3 4 1 2	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Gi1/1 Gi1/2
1783-BM06SGA	switch administré à 6 ports (4 ports Ethernet, 2 emplacements SFP Gigabit), firmware complet	1 2 3 4 1 2	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Gi1/1 Gi1/2
1783-BMS06TGL	switch administré à 6 ports (4 ports Ethernet, 2 ports Gigabit), firmware complet	1 2 3 4 1 2	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Gi1/1 Gi1/2
1783-BMS06TGA	switch administré à 6 ports (4 ports Ethernet, 2 ports Gigabit), firmware complet	1 2 3 4 1 2	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Gi1/1 Gi1/2

Tableau 2 - Numérotation des ports (suite)

Référence	Description	Numérotation des ports sur les étiquettes du switch	Numérotation des ports dans le fichier config.text
1783-BMS10CL	switch administré à 10 ports (8 ports Ethernet, 2 ports mixtes), firmware version légère	1 2 3 4 5 6 7 8 9 10	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6 Fa1/7 Fa1/8 Fa1/9 Fa1/10
1783-BMS10CA	switch administré à 10 ports (8 ports Ethernet, 2 ports mixtes), firmware complet	1 2 3 4 5 6 7 8 9 10	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6 Fa1/7 Fa1/8 Fa1/9 Fa1/10
1783-BMS10CGL	switch administré à 10 ports (8 ports Ethernet, 2 ports mixtes Gigabit), firmware version légère	1 2 3 4 5 6 7 8 1 2	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6 Fa1/7 Fa1/8 Gi1/1 Gi1/2
1783-BMS10CGA	switch administré à 10 ports (8 ports Ethernet, 2 ports mixtes Gigabit), firmware complet	1 2 3 4 5 6 7 8 1 2	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6 Fa1/7 Fa1/8 Gi1/1 Gi1/2
1783-BMS10CGN	switch administré à 10 ports (8 ports Ethernet, 2 ports mixtes Gigabit), firmware complet, NAT	1 2 3 4 5 6 7 8 1 2	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6 Fa1/7 Fa1/8 Gi1/1 Gi1/2

Tableau 2 - Numérotation des ports (suite)

Référence	Description	Numérotation des ports sur les étiquettes du switch	Numérotation des ports dans le fichier config.text
1783-BMS10CGP	switch administré à 10 ports (8 ports Ethernet, 2 ports mixtes Gigabit), firmware complet, PTP	1 2 3 4 5 6 7 8 1 2	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6 Fa1/7 Fa1/8 Gi1/1 Gi1/2
1783-BMS12T4E2CGNK	switch administré à 18 ports (12 ports Ethernet, 4 ports PoE/PoE+, 2 ports mixtes Gigabit), firmware complet, NAT, revêtement enrobant	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 1 2	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6 Fa1/7 Fa1/8 Fa1/9 Fa1/10 Fa1/11 Fa1/12 Fa1/13 Fa1/14 Fa1/15 Fa1/16 Gi1/1 Gi1/2
1783-BMS12T4E2CGP	switch administré à 18 ports (12 ports Ethernet, 4 ports PoE/PoE+, 2 ports mixtes Gigabit), firmware complet	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 1 2	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6 Fa1/7 Fa1/8 Fa1/9 Fa1/10 Fa1/11 Fa1/12 Fa1/13 Fa1/14 Fa1/15 Fa1/16 Gi1/1 Gi1/2

Tableau 2 - Numérotation des ports (suite)

Référence	Description	Numérotation des ports sur les étiquettes du switch	Numérotation des ports dans le fichier config.text
1783-BMS12T4E2CGL	switch administré à 18 ports (12 ports Ethernet, 4 ports PoE/PoE+, 2 ports mixtes Gigabit), firmware version légère	1	Fa1/1
		2	Fa1/2
		3	Fa1/3
		4	Fa1/4
		5	Fa1/5
		6	Fa1/6
		7	Fa1/7
		8	Fa1/8
		9	Fa1/9
		10	Fa1/10
		11	Fa1/11
		12	Fa1/12
		13	Fa1/13
		14	Fa1/14
		15	Fa1/15
		16	Fa1/16
		1	Gi1/1
		2	Gi1/2
1783-BMS20CL	switch administré à 20 ports (16 ports Ethernet, 2 emplacements SFP, 2 ports mixtes), firmware version légère	1	Fa1/1
		2	Fa1/2
		3	Fa1/3
		4	Fa1/4
		5	Fa1/5
		6	Fa1/6
		7	Fa1/7
		8	Fa1/8
		9	Fa1/9
		10	Fa1/10
		11	Fa1/11
		12	Fa1/12
		13	Fa1/13
		14	Fa1/14
		15	Fa1/15
		16	Fa1/16
		17	Fa1/17
		18	Fa1/18
		19	Fa1/19
		20	Fa1/20
1783-BMS20CA	switch administré à 20 ports (16 ports Ethernet, 2 emplacements SFP, 2 ports mixtes), firmware complet	1	Fa1/1
		2	Fa1/2
		3	Fa1/3
		4	Fa1/4
		5	Fa1/5
		6	Fa1/6
		7	Fa1/7
		8	Fa1/8
		9	Fa1/9
		10	Fa1/10
		11	Fa1/11
		12	Fa1/12
		13	Fa1/13
		14	Fa1/14
		15	Fa1/15
		16	Fa1/16
		17	Fa1/17
		18	Fa1/18
		19	Fa1/19
		20	Fa1/20

Tableau 2 - Numérotation des ports (suite)

Référence	Description	Numérotation des ports sur les étiquettes du switch	Numérotation des ports dans le fichier config.text
1783-BMS20CGL	switch administré à 20 ports (16 ports Ethernet, 2 emplacements SFP, 2 ports mixtes Gigabit), firmware version légère	1	Fa1/1
		2	Fa1/2
		3	Fa1/3
		4	Fa1/4
		5	Fa1/5
		6	Fa1/6
		7	Fa1/7
		8	Fa1/8
		9	Fa1/9
		10	Fa1/10
		11	Fa1/11
		12	Fa1/12
		13	Fa1/13
		14	Fa1/14
		15	Fa1/15
		16	Fa1/16
		17	Fa1/17
		18	Fa1/18
		1	Gi1/1
		2	Gi1/2
1783-BMS20CGN	switch administré à 20 ports (16 ports Ethernet, 2 emplacements SFP, 2 ports mixtes Gigabit), firmware complet, NAT	1	Fa1/1
		2	Fa1/2
		3	Fa1/3
		4	Fa1/4
		5	Fa1/5
		6	Fa1/6
		7	Fa1/7
		8	Fa1/8
		9	Fa1/9
		10	Fa1/10
		11	Fa1/11
		12	Fa1/12
		13	Fa1/13
		14	Fa1/14
		15	Fa1/15
		16	Fa1/16
		17	Fa1/17
		18	Fa1/18
		1	Gi1/1
		2	Gi1/2
1783-BMS20CGP	switch administré à 20 ports (16 ports Ethernet, 2 emplacements SFP, 2 ports mixtes Gigabit), firmware complet, PTP	1	Fa1/1
		2	Fa1/2
		3	Fa1/3
		4	Fa1/4
		5	Fa1/5
		6	Fa1/6
		7	Fa1/7
		8	Fa1/8
		9	Fa1/9
		10	Fa1/10
		11	Fa1/11
		12	Fa1/12
		13	Fa1/13
		14	Fa1/14
		15	Fa1/15
		16	Fa1/16
		17	Fa1/17
		18	Fa1/18
		1	Gi1/1
		2	Gi1/2

Tableau 2 - Numérotation des ports (suite)

Référence	Description	Numérotation des ports sur les étiquettes du switch	Numérotation des ports dans le fichier config.text
1783-BMS20CGPK	switch administré à 20 ports (16 ports Ethernet, 2 emplacements SFP, 2 ports mixtes Gigabit), firmware complet, PTP, revêtement enrobant	1	Fa1/1
		2	Fa1/2
		3	Fa1/3
		4	Fa1/4
		5	Fa1/5
		6	Fa1/6
		7	Fa1/7
		8	Fa1/8
		9	Fa1/9
		10	Fa1/10
		11	Fa1/11
		12	Fa1/12
		13	Fa1/13
		14	Fa1/14
		15	Fa1/15
		16	Fa1/16
		17	Fa1/17
		18	Fa1/18
		1	Gi1/1
		2	Gi1/2

Macro globale

Une fois Express Setup terminée, tel que décrit page 51, le switch exécute une macro globale (ab-globale). Cette macro configure le switch pour les applications d'automatisation industrielle typiques qui utilisent le protocole EtherNet/IP. Cette macro définit plusieurs paramètres, y compris les réglages principaux suivants :

- Activer la surveillance et l'interrogation IGMP
- Activer le CIP
- Configurer les paramètres QoS et classer le trafic CIP, le trafic PTP et tout autre trafic (ne s'applique pas aux switchs dont le firmware allégé a été révisé)
- Prise en charge des alarmes et des notifications SNMP et SYSLOG
- Prise en charge du protocole RSTP (Rapid Spanning Tree), de la protection BPDU, du filtrage BPDU et de la protection de la boucle

Si vous n'exécutez pas Express Setup pour initialiser le switch, la macro globale n'est pas exécutée. Vous pouvez utiliser la CLU pour exécuter la macro globale.

Smartports

Les smartports sont des configurations recommandées pour les ports du switch. Ces configurations, appelées rôles des ports, optimisent les connexions du switch et garantissent la sécurité, la qualité de transmission et la fiabilité du trafic à partir des ports. Les rôles de port permettent également d'éviter les erreurs de configuration des ports.

CONSEIL Utilisez des rôles de smartport immédiatement après l'installation initiale du switch pour configurer correctement les ports du switch avant qu'ils ne se connectent aux dispositifs.

Optimiser les ports grâce aux rôles des ports smartport

Les rôles des ports décrits dans le Tableau 3 reposent sur le type de dispositifs à connecter aux ports du switch. Par exemple, le rôle de port « ordinateur de bureau pour l'automatisation » est spécialement dédié aux ports du switch à connecter aux ordinateurs de bureau et aux ordinateurs portables.

Rôles de smartport personnalisés

Les switchs Stratix 5700 vous permettent de créer et de modifier jusqu'à 10 rôles de smartport personnalisés pour de nombreuses applications personnalisées. Vous pouvez importer ou exporter des rôles de smartport personnalisés uniquement si vous utilisez le navigateur Internet Mozilla Firefox, version 3.6 ou supérieure. Par défaut, les ports de switch sont configurés sur le rôle de port None (aucun).

Tableau 3 - Rôles des smartports

Rôle du port	Description
Automation Device (dispositif d'automatisation)	Appliquez ce rôle aux ports à connecter aux dispositifs EtherNet/IP (protocole Ethernet industriel). Il peut être utilisé pour les dispositifs d'automatisation industrielle comme les automates et les entrées/sorties : • Le port est configuré en mode Access : • La sécurité de port prend en charge un seul MAC ID. • Gestion de la file d'attente optimisée pour le trafic CIP.
Multiport Automation Device (dispositif d'automatisation multiport)	Appliquez ce rôle aux ports connectés aux dispositifs EtherNet/IP multiport, comme les dispositifs EtherNet/IP multiport installés de manière linéaire ou en série, le module 1783-ETAP (à ne raccorder qu'au port du dispositif), les switchs non administrés (comme le Stratix 2000™) et les switchs administrés avec le protocole RSTP (Remote Spanning Tree) désactivé : • Le port est configuré en mode Access. • Aucune sécurité de port. • Gestion de la file d'attente optimisée pour le trafic CIP.
Desktop for Automation (ordinateur pour l'automatisation)	Appliquez ce rôle aux ports à connecter aux dispositifs de bureau, comme les ordinateurs de bureau, les stations de travail, les ordinateurs portables et d'autres hôtes côté client : • Le port est configuré en mode Access. • PortFast activé. • La sécurité de port prend en charge un seul MAC ID. Ce rôle n'est pas adapté aux ports à connecter à des switchs, des routeurs ou des points d'accès.
Virtual Desktop for Automation (ordinateur virtuel pour l'automatisation)	Appliquez ce rôle aux ports connectés aux ordinateurs exécutant le logiciel de virtualisation. Vous pouvez l'utiliser avec les dispositifs exécutant jusqu'à deux adresses MAC : • Le port est configuré en mode Access. • PortFast est activé. • La sécurité du port prend en charge deux MAC ID. **IMPORTANT :** n'appliquez pas le bureau virtuel du rôle d'automatisation aux ports connectés aux switchs, routeurs ou points d'accès.
Switch for Automation (switch pour l'automatisation)	Appliquez ce rôle aux ports à connecter aux autres switchs avec le protocole Spanning Tree activé. Le port est défini en mode Trunk.
Router for Automation (routeur pour l'automatisation)	Appliquez ce rôle aux ports à connecter aux routeurs ou switchs de couche 3 avec service d'acheminement activé.

Tableau 3 - Rôles des smartports (suite)

Rôle du port	Description
Phone for Automation (téléphone pour l'automatisation)	Appliquez ce rôle aux ports à connecter aux téléphones IP. Un dispositif de bureau, tel qu'un ordinateur, peut être branché au téléphone IP. Le téléphone IP et l'ordinateur connecté ont accès au réseau par l'intermédiaire du port : • Le port est défini en mode Trunk. • La sécurité de port prend en charge trois MAC ID vers ce port. Ce rôle donne la priorité au trafic téléphonique plutôt qu'au trafic de données générales afin de garantir une bonne réception vocale sur les téléphones IP.
Wireless for Automation (sans fil pour l'automatisation)	Appliquez ce rôle aux ports à connecter aux points d'accès sans fil. Le point d'accès peut fournir l'accès au réseau à 30 utilisateurs sans fil au maximum.
Port Mirroring (port miroir)	Appliquez ce rôle aux ports devant être surveillés par un analyseur de réseau. Pour plus d'informations sur la mise en miroir de ports, voir Mise en miroir de ports à la page 92.
None (aucun)	Appliquez ce rôle aux ports si vous ne souhaitez pas appliquer un rôle de smartport spécialisé au port. Ce rôle peut être utilisé pour les connexions à tout dispositif, y compris les dispositifs dans les rôles décrits ci-dessus.
CS1…CS10	Rôles de smartport personnalisés. Vous pouvez créer un rôle de port personnalisé avec un nom défini par l'utilisateur. Reportez-vous au Chapitre 4, Gestion du switch via l'interface Internet de Device Manager, pour plus d'informations sur la création des rôles de smartport personnalisés.

Prévention des incompatibilités de smartports

Une incompatibilité de smartport se produit lorsqu'un dispositif connecté ne correspond pas au rôle de smartport appliqué au port du switch. Les incompatibilités peuvent avoir des effets néfastes sur votre réseau et vos dispositifs.

Les incompatibilités peuvent entraîner les conditions suivantes :

- Affecter le comportement du dispositif connecté
- Réduire les performances du réseau (réduire le niveau de qualité de service [QoS]) sur le CIP, les performances vocales, sans fil, du switch et du trafic du routeur
- Réduire les restrictions de l'accès invité sur le réseau
- Réduire la protection contre les attaques par déni de service (DoS) sur le réseau
- Désactiver ou fermer le port

Nous recommandons de toujours vérifier quel rôle de smartport est appliqué à un port avant d'y raccorder un dispositif ou d'y reconnecter des dispositifs.

Power over Ethernet (PoE)

Les switchs dotés de ports PoE sont configurables par logiciel et fournissent les caractéristiques suivantes :

- Prise en charge des dispositifs (PoE) compatibles IEEE 802.3af.
- Prise en charge de la norme IEEE 802.3at, type 2 (PoE+) qui augmente de 15,4 à 30 W par port, la puissance disponible consommable par les dispositifs alimentés.
- Détection automatique et budgétisation de l'alimentation. Le switch gère un bilan d'alimentation, surveille et suit les demandes d'alimentation et alloue l'alimentation seulement quand elle est disponible.

- Alimentation des dispositifs alimentés conforme à la norme IEEE 802.3af et des dispositifs pré-standard Cisco connectés si le switch détecte l'absence d'alimentation dans le circuit.

- Prise en charge du protocole CDP (Cisco Discovery Protocol) avec consommation électrique. Cette caractéristique s'applique uniquement lors de l'utilisation des switchs avec des dispositifs finaux Cisco. Le dispositif final Cisco alimenté notifie le switch de la quantité d'électricité consommée. Le switch peut ainsi fournir ou couper l'alimentation à partir du port PoE.

- Prise en charge de la gestion intelligente de l'énergie Cisco. Un dispositif final Cisco alimenté et le switch négocient un niveau convenu de consommation électrique par l'intermédiaire de messages CDP de négociation de l'alimentation. La négociation permet à un dispositif de puissance élevée consommant plus de 7 W de fonctionner dans son mode de consommation le plus élevé. Le dispositif alimenté démarre tout d'abord en mode de faible puissance, consomme moins de 7 W et négocie pour obtenir assez de puissance pour fonctionner en mode de puissance élevée. Le dispositif bascule en mode de puissance élevée uniquement lorsqu'il reçoit une confirmation du switch.

  La gestion intelligente de l'énergie Cisco est rétrocompatible avec le protocole CDP avec consommation électrique. Le module répond en tenant compte du message CDP reçu. Le protocole CDP n'est pas pris en charge par les dispositifs alimentés tiers, le module utilise la classification IEEE pour déterminer la consommation électrique du dispositif.

Détection du dispositif alimenté et allocation de puissance initiale

Un switch détecte un dispositif alimenté lorsqu'un port doté de la fonctionnalité PoE est actif, la fonctionnalité PoE est activée (par défaut) et le dispositif connecté n'est pas alimenté par une autre source d'alimentation.

Après la détection du dispositif, le switch détermine les exigences électriques du dispositif en fonction de son type :

- Le switch assigne le dispositif IEEE compatible 802.3 af/at détecté à une classe de consommation électrique. En fonction de la puissance disponible au niveau du budget d'alimentation, le switch détermine si un port PoE peut être alimenté. Le tableau ci-dessous répertorie ces niveaux.

Tableau 4 - Classifications de l'alimentation selon la norme IEEE

Classe	Alimentation fournie par port, max.
0 (classe dont l'état est inconnu)	15,4 W
1	4 W
2	7 W
3	15,4 W
4	Dispositifs PoE+ 30 W uniquement

- Un dispositif alimenté pré-standard Cisco n'indique pas ses besoins électriques lorsque le switch le détecte. Un port non PoE+ alloue initialement 15,4 W comme attribution de puissance initiale pour le bilan de puissance. Un port configuré pour un switch PoE+ alloue 30 W.

  L'allocation de puissance initiale correspond à la quantité de puissance maximale que requiert un dispositif alimenté. Le switch alloue initialement cette quantité de puissance lorsqu'il détecte et alimente le dispositif alimenté. Comme le switch reçoit des messages CDP du dispositif alimenté et que le dispositif alimenté négocie les niveaux de puissance avec le module par l'intermédiaire des messages CDP de négociation de l'alimentation, l'allocation de puissance initiale peut être ajustée.

Le switch surveille et suit les demandes d'alimentation et attribue l'alimentation seulement quand elle est disponible. Le switch suit le bilan d'alimentation qui correspond à la quantité de puissance disponible sur chaque port PoE. Le switch effectue les calculs de puissance lorsqu'un port se voit allouer ou refuser une puissance pour maintenir le bilan d'alimentation à jour.

Une fois la puissance appliquée à un port PoE, le switch utilise le protocole CDP (si ce dernier est pris en charge par le dispositif final Cisco alimenté) pour déterminer le besoin réel de consommation électrique des dispositifs alimentés connectés et ajuste le bilan d'alimentation en conséquence. Le switch traite une demande et autorise ou refuse l'alimentation. Si la demande est accordée, le switch met à jour le bilan d'alimentation. Si la demande est refusée, le switch vérifie que l'alimentation du port est désactivée, génère un message syslog et met à jour les voyants d'état. Les dispositifs alimentés peuvent également négocier avec le module pour bénéficier de plus de puissance.

Si le switch détecte un défaut causé par une sous-tension, une surtension, une surchauffe, un défaut de l'oscillateur ou un court-circuit, il coupe l'alimentation du port, génère un message syslog et met à jour le bilan d'alimentation et les voyants d'état.

Modes de gestion de l'alimentation

Les ports PoE prennent en charge les modes suivants :

- Auto (par défaut) - le port détecte automatiquement si le dispositif connecté requiert une alimentation. Il s'agit du mode par défaut.
  Si le port détecte un dispositif alimenté connecté et que le module a assez de puissance, il autorise l'alimentation, met à jour le bilan d'alimentation, met le port sous tension sur la base « premier arrivé, premier servi » et met à jour les voyants d'état.

  Si assez de puissance est disponible pour tous les dispositifs alimentés connectés au switch, tous les dispositifs sont mis sous tension. Si la puissance disponible n'est pas suffisante pour prendre en charge tous les dispositifs connectés et si un dispositif est déconnecté et reconnecté tandis que d'autres dispositifs sont en attente d'alimentation, il est impossible de déterminer pour quels dispositifs l'alimentation est autorisée ou refusée.

Si la puissance autorisée dépasse le bilan d'alimentation du système, le switch refuse d'alimenter le port, vérifie que le port est désactivé, génère un message syslog et met à jour les voyants d'état. Après avoir refusé l'alimentation, le switch revérifie périodiquement le bilan d'alimentation et continue de tenter d'accepter la demande d'alimentation.

Si un dispositif alimenté par le switch est ensuite connecté à une prise murale, le switch peut continuer d'alimenter le dispositif. Le switch peut continuer de signaler qu'il alimente toujours le dispositif si ce dernier est alimenté par le switch ou par une source d'alimentation c.a.

Si un dispositif alimenté est retiré, le switch détecte automatiquement la déconnexion et met le port hors tension. Vous pouvez connecter un dispositif non alimenté sans l'endommager.

Vous pouvez spécifier la puissance maximale (en watts) que le port peut prendre en charge. Si la puissance maximale conforme à la norme IEEE du dispositif alimenté est supérieure à la valeur maximale configurée, le switch n'alimente pas le port. Si le switch alimente un dispositif final Cisco alimenté, mais que le dispositif alimenté demande ultérieurement par l'intermédiaire de messages CDP une puissance supérieure à la valeur maximale configurée, le switch bascule le port hors tension. La puissance allouée au dispositif alimenté est réintroduite dans le bilan global d'alimentation. Si vous ne spécifiez pas de puissance, le switch fournit la valeur maximale.

- Static- le switch alloue par défaut une puissance au port même si aucun dispositif alimenté n'est connecté et garantit que la puissance est disponible au niveau du port. Le switch alloue la puissance maximale configurée pour le port ; cette valeur n'est jamais ajustée par l'intermédiaire de la classe IEEE ou des messages CDP provenant d'un dispositif final Cisco alimenté. Comme la puissance est allouée par défaut, tout dispositif alimenté qui utilise une puissance inférieure ou égale à la puissance maximale est systématiquement alimenté lorsqu'il est connecté au port statique. Le port ne respecte plus le modèle « premier arrivé, premier servi ».

  Toutefois, si la classe IEEE du dispositif alimenté est supérieure à la puissance maximale, le switch n'alimente pas le dispositif. Si le switch apprend à travers les messages CDP qu'un dispositif final Cisco alimenté requiert une puissance supérieure à la puissance maximale, le dispositif alimenté est mis hors tension.

  Si vous ne spécifiez pas de puissance, le switch alloue par défaut la valeur maximale. Le switch alimente le port uniquement s'il détecte un dispositif alimenté. Utilisez le paramètre statique sur une interface avec une priorité élevée.

- Off - le switch désactive la détection du dispositif alimenté et n'alimente jamais le port PoE même si un dispositif non alimenté est connecté. Utilisez ce mode uniquement lorsque vous souhaitez vous assurer de ne jamais alimenter un port PoE afin que ce dernier serve uniquement de port de données.

Allocation d'une puissance maximale (coupure d'alimentation) à un port PoE

Le switch détermine la coupure d'alimentation d'un port PoE dans cet ordre.

1. Manuellement lorsque vous configurez le niveau de puissance pour budgétiser le port.
2. Manuellement lorsque vous configurez le niveau de puissance qui limite la puissance allouée au port.
3. Automatiquement lorsque le switch définit la consommation électrique du dispositif à l'aide de la classification IEEE et de la négociation de l'alimentation LLDP ou CDP.

Si vous ne configurez pas manuellement la valeur de coupure d'alimentation, le switch peut déterminer automatiquement cette valeur à l'aide de la négociation de l'alimentation CDP en cas de connexion à un dispositif final Cisco. Si le switch ne peut pas déterminer cette valeur en utilisant l'une de ces méthodes, il utilise la valeur par défaut de 15,4 W.

Avec PoE+, si vous ne configurez pas manuellement la valeur de coupure d'alimentation, le switch la détermine automatiquement à l'aide de la classification IEEE du dispositif et de la négociation de l'alimentation LLDP ou CDP avec un dispositif de blocage de Cisco. Si CDP ou LLDP est désactivé, la valeur par défaut de 30 W est appliquée. Toutefois, sans CDP ou LLDP, le switch ne permet pas aux dispositifs de consommer plus de 15,4 W, car des valeurs de 15 400 à 30 000 mW sont allouées en fonction des demandes CDP ou LLDP uniquement. Si un dispositif alimenté consomme plus de 15,4 W sans négociation CDP ou LLDP, le dispositif peut ne pas respecter la limite maximale de courant ; la consommation d'un courant supérieur à la valeur maximale supportée peut entraîner un défaut. Le port conserve l'état de défaut pendant un certain temps avant d'essayer de basculer sous tension à nouveau. Si le port supporte en permanence une puissance supérieure à 15,4 W, le cycle se répète.

Valeurs de consommation électrique

Vous pouvez configurer l'allocation de puissance initiale et l'allocation de puissance maximale d'un port. Toutefois, ces valeurs correspondent uniquement aux valeurs de configuration qui déterminent quand la switch alimente ou n'alimente pas le port PoE. L'allocation de puissance maximale est différente de la consommation électrique réelle du dispositif alimenté. Lorsque vous définissez manuellement l'allocation de puissance maximale, vous devez considérer la perte de puissance au niveau du câble entre le port et le dispositif alimenté. La coupure d'alimentation est la somme de la consommation électrique nominale du dispositif alimenté et d'une perte de puissance maximale au niveau du câble.

La quantité réelle d'alimentation consommée par un dispositif alimenté sur un port PoE correspond à la valeur de coupure de l'alimentation, plus un facteur d'étalonnage de 500 mW (0,5 W). La valeur de coupure réelle est approximative et varie par rapport à la valeur configurée en fonction d'un pourcentage de la valeur configurée. Par exemple, si la coupure d'alimentation configurée est configurée sur 12 W, la valeur de coupure réelle est de 11,4 W, soit 0,05 % de moins que la valeur configurée.

Comme le switch prend en charge des alimentations amovibles externes pour PoE/PoE+ et peut configurer le bilan par alimentation utilisée, la quantité totale de puissance disponible pour les dispositifs alimentés varie en fonction de la configuration des alimentations :

- Si une alimentation est retirée et remplacée par une nouvelle alimentation moins puissante et que le module n'a pas assez de puissance pour les dispositifs alimentés, le switch refuse d'alimenter les ports PoE en mode automatique dans l'ordre décroissant des numéros de port. Si le switch n'a toujours pas assez de puissance, il refuse d'alimenter les ports PoE en mode statique dans l'ordre décroissant des numéros de port.

- Si la novelle alimentation prend en charge plus de puissance que la précédente, le switch possède désormais plus de puissance et autorise l'alimentation des ports PoE en mode statique dans l'ordre croissant des numéros de port. Si de la puissance est encore disponible, le switch accepte d'alimenter les ports PoE en mode automatique dans l'ordre croissant des numéros de port.

IMPORTANT Pour répartir l'alimentation avec précision, la puissance totale de l'alimentation doit être configurée manuellement via l'interface Internet de Device Manager ou CIP.

VLAN

Un réseau local virtuel (VLAN) est un segment logique des utilisateurs du réseau et des ressources regroupés par fonction, par équipe ou par application. Cette segmentation ne tient pas compte de l'emplacement physique des utilisateurs et des ressources. Par exemple, les VLAN peuvent être basés sur les services de votre entreprise ou des ensembles d'utilisateurs qui communiquent plus fréquemment entre eux.

Le switch est livré avec un VLAN par défaut auquel appartiennent tous les ports du switch au départ. Le switch prend en charge un maximum de 255 VLAN, y compris le VLAN par défaut.

Chaque VLAN est identifié par son nom et son numéro d'identification (ID). Le VLAN par défaut s'appelle default. L'ID peut être compris entre 1 et 1001 et entre 1005 et 4094, 1 correspondant à l'ID par défaut.

Vous pouvez assigner les ports du switch au VLAN par défaut ou à des VLAN que vous avez créés. Le VLAN par défaut seul peut être suffisant suivant la taille et les exigences de votre réseau. Nous vous recommandons de commencer par déterminer vos besoins en matière de VLAN avant de les créer.

Avec des smartports personnalisés, vous pouvez spécifier le type de VLAN à mettre en œuvre sur ce port.

Le VLAN par défaut est également le VLAN de gestion. Après l'installation initiale, vous pouvez créer des VLAN et désigner n'importe quel VLAN comme le VLAN de gestion. Le VLAN de gestion fournit un accès administratif au switch. Vous devez attribuer l'un des ports du switch au VLAN de gestion. Dans le cas contraire, vous n'avez pas d'accès administratif au switch. Initialement, tous les ports sont assignés au VLAN de gestion.

Vous pouvez assigner tous les ports, indépendamment de leur rôle de smartport, au VLAN par défaut (default).

Isoler le trafic et les utilisateurs

À l'aide des VLAN, vous pouvez isoler différents types de trafic, comme le trafic vocal et de données, afin de préserver la qualité de la transmission et de minimiser le trafic excédentaire sur les segments logiques. Vous pouvez également utiliser des VLAN pour isoler les différents types d'utilisateurs. Vous pouvez limiter la diffusion de données spécifiques à des groupes de travail logiques spécifiques à des fins de sécurité, pour conserver les informations sur le salaire des employés uniquement sur les dispositifs d'un VLAN créé pour les communications liées à la paie, par exemple.

L'utilisation de VLAN permet également de réduire la quantité d'effort administratif requis pour examiner en permanence les demandes de ressources réseau.

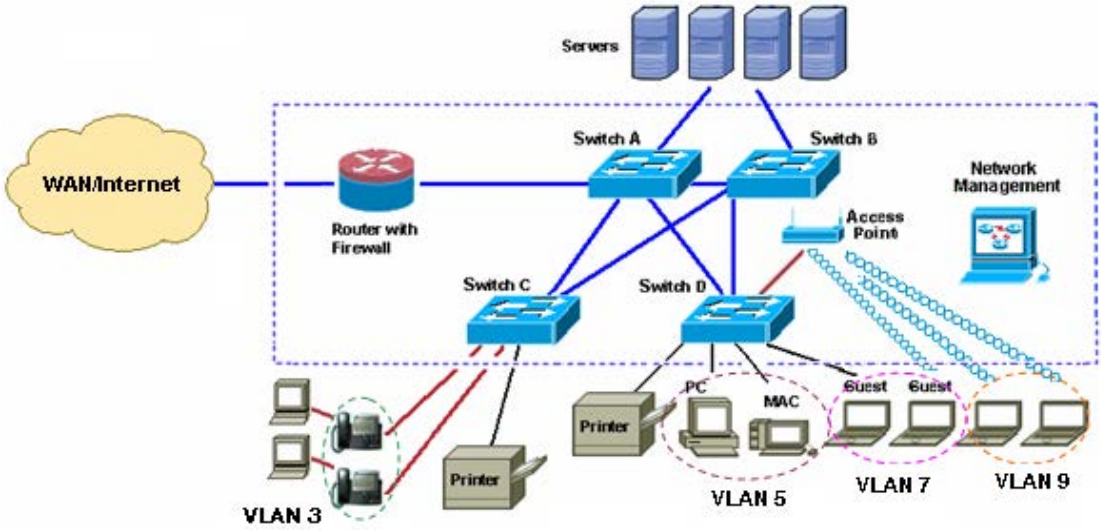
Les VLAN isolent les différentes parties de votre réseau. Par conséquent, les dispositifs qui sont reliés aux ports du switch dans le même VLAN (utilisateurs du réseau dans le même VLAN) peuvent communiquer entre eux uniquement et partager les mêmes données.

Les dispositifs connectés aux ports du switch de différents VLAN ne peuvent pas communiquer entre eux par l'intermédiaire du switch, sauf si le switch est configuré pour le routage. Un switch Stratix 5700, un routeur ou un switch de couche 3 doit être configuré pour activer le routage entre les VLAN (routage inter-VLAN) et des politiques de sécurité supplémentaires doivent être définies.

Si votre réseau utilise également un serveur DHCP, vérifiez que le serveur est accessible par les dispositifs de tous les VLAN.

La figure suivante est un exemple de réseau qui utilise des VLAN basés sur des trafics réseau et des utilisateurs du réseau différents. L'organisation d'un réseau autour de ces facteurs contribue à définir la taille et la composition des VLAN dans le réseau.

Figure 1 - Exemple de VLAN



Isoler différents types de trafic

Isoler le trafic de données du trafic sensible aux délais, comme le trafic vocal, augmente la qualité de la transmission vocale. Dans l'illustration ci-dessus, les ports du switch connectés à des téléphones IP appartiennent au VLAN 3, un VLAN qui est configuré pour fournir des services de voix sur IP (VoIP) sur ces connexions, ce qui signifie que le trafic vocal est prioritaire sur le trafic de données IP régulier. Le trafic vocal transitant par un serveur PBX-IP via un téléphone ou un service de téléphonie IP est prioritaire sur le trafic provenant de dispositifs de bureau connectés à des téléphones IP.

Pour isoler davantage le trafic de données du trafic vocal, le trafic de données provenant des dispositifs de bureau connectés peut être assigné à un VLAN distinct.

Regrouper les utilisateurs

Le réseau illustré Figure 1 fournit un accès à trois types d'utilisateurs du réseau :

- Employés filaires
- Employés sans fil
- Visiteurs de l'entreprise filaires ou sans fil

Chaque type d'utilisateur requiert des niveaux d'accès différents au réseau de l'entreprise. Les VLAN et les politiques de sécurité d'un routeur ou d'un switch de couche 3 permettent d'appliquer des privilèges et des restrictions aux différents types de l'utilisateur.

Reportez-vous à la Figure 1 à la page 71 :

- Le VLAN 5 offre un accès de niveau employé aux ressources de l'entreprise. Ce type d'accès au réseau nécessite une connexion directe à des ports spécifiques du switch.

- Le VLAN 7 offre uniquement accès à Internet aux visiteurs de l'entreprise. Les visiteurs avec une connexion filaire ou sans fil aux ports du switch sont assignés à ce VLAN, ce qui limite automatiquement leur accès à Internet uniquement.

- Le VLAN 9, dont un ou plusieurs ports de switch sont connectés au point d'accès sans fil, applique des politiques de sécurité visant à identifier l'utilisateur sans fil (par exemple, comme un employé ou un invité) et à déterminer ce que l'utilisateur peut faire sur le réseau (par exemple, accéder uniquement à Internet ou à d'autres ressources du réseau).

Surveillance et interrogation IGMP

Les switchs de couche 2 peuvent utiliser la surveillance IGMP pour limiter la prolifération du trafic de multidiffusion en configurant de manière dynamique les interfaces de couche 2 de sorte que le trafic de multidiffusion soit uniquement transféré aux interfaces associées aux dispositifs IP de multidiffusion. Comme son nom l'indique, la surveillance IGMP requiert que le switch LAN surveillance les transmissions IGMP entre l'hôte et le routeur et assure le suivi des groupes de multidiffusion et des ports membres. Lorsque le switch reçoit un rapport IGMP d'un hôte d'un groupe particulier de multidiffusion, il ajoute le numéro de port hôte à l'entrée de la table de transfert. Lorsque le switch reçoit d'un hôte un message IGMP de départ du groupe, il supprime le port hôte de l'entrée de la table. Il supprime également périodiquement les entrées s'il ne reçoit pas de rapports d'appartenance IGMP des clients de multidiffusion.

Le routeur de multidiffusion envoie des demandes générales périodiques à tous les VLAN. Tous les hôtes intéressés par ce trafic de multidiffusion envoient des demandes d'accès et sont ajoutés à l'entrée de la table de transfert. Le switch crée une entrée par VLAN dans la table de transfert avec multidiffusion par IP de la surveillance IGMP pour chaque groupe dont il reçoit une demande d'accès IGMP.

Le switch prend en charge le pont à partir du groupe de multidiffusion par IP plutôt que les groupes à partir des adresses MAC. Avec les groupes de multidiffusion à partir d'une adresse MAC, si une adresse IP configurée transite (alias) par une adresse MAC précédemment configurée ou une adresse MAC de multidiffusion réservée (plage 224.0.0.xxx), la commande échoue. Comme le switch utilise des groupes de multidiffusion par IP, il n'y a pas de problème de dénomination d'adresse.

256 est le nombre par défaut de groupes de multidiffusion pris en charge par les switchs. Si vous dépassez 180 groupes de multidiffusion, nous vous recommandons de basculer sur le modèle d'acheminement SDM à l'aide de l'interface CLI.

Les groupes de multidiffusion par IP mémorisés par la surveillance IGMP sont dynamiques. Si vous spécifiez qu'une adresse de groupe de multidiffusion appartient de manière statique à un groupe, votre paramètre remplace toute manipulation automatique de la surveillance IGMP. La liste d'appartenance à un groupe de multidiffusion peut consister en la configuration de l'utilisateur et en la configuration mémorisée par la surveillance IGMP. Les adresses de multidiffusion par IP utilisées par le réseau EtherNet/IP pour le trafic d'E/S sont mémorisées par le switch.

Le protocole IGMP mis en œuvre sur le switch est IGMP V2. Cette version est rétro-compatible avec les switchs exécutant IGMP V1. Le switch intègre une fonction d'interrogation et la macro globale prend en charge la surveillance et l'interrogation IGMP.

Protocole STP (Spanning Tree Protocol)

Le protocole STP (protocole de l'arbre maximal) est un protocole de gestion de liaison de couche 2 qui assure la redondance des chemins tout en évitant les boucles de réseau. Pour qu'un réseau Ethernet de couche 2 fonctionne correctement, seul un chemin actif peut exister entre deux stations. Plusieurs chemins actifs entre les stations finales créent des boucles dans le réseau. Si une boucle existe dans le réseau, les stations finales peuvent recevoir des messages en double. Les switchs peuvent également mémoriser les adresses MAC des stations finales sur plusieurs interfaces de couche 2. Ces conditions créent un réseau instable. Le fonctionnement de type Spanning Tree est transparent pour les stations finales qui ne peuvent pas détecter si elles sont connectées à un seul segment de réseau local ou à un ensemble commuté de plusieurs segments du réseau local.

Le protocole STP utilise un algorithme de l'arbre maximal pour sélectionner un seul switch d'un réseau connecté de manière redondante comme racine de l'arbre maximal. L'algorithme calcule le meilleur parcours sans boucle à travers un réseau commuté de couche 2 en assignant un rôle à chaque port en fonction du rôle du port dans la topologie active :

- Racine — port de transfert choisi pour la topologie de l'arbre maximal
- Désigné — port de transfert choisi pour chaque segment commuté du réseau local
- Rechange — port bloqué fournissant un autre chemin d'accès au pont racine de l'arbre maximal
- Sauvegarde — port bloqué dans une configuration en boucle

Le switch dont tous les ports ont reçu le rôle « désigné » ou le rôle « sauvegarde » est le switch racine. Le switch dont au moins l'un des ports a reçu le rôle « désigné » est appelé le switch désigné.

L'arbre maximal force le passage des chemins de données redondants dans un état de veille (bloqué). Si un segment du réseau de l'arbre maximal échoue et qu'il existe un chemin redondant, l'algorithme de l'arbre maximal recalcule la topologie de l'arbre maximal et active le chemin d'accès en veille. Les switchs envoient et reçoivent les trames de l'arbre maximal, appelées unités de données de protocole de pont (BPDU) à intervalles réguliers. Les switchs ne transmettent pas ces trames, mais les utilisent pour construire un chemin d'accès sans boucle. Les BPDU contiennent des informations sur le switch d'émission et ses ports, y compris les adresses MAC et du switch, la priorité du switch, la priorité du port et le coût du chemin d'accès. L'arbre maximal utilise ces informations pour choisir le switch racine et le port racine du réseau commuté, ainsi que le port racine et le port désigné de chaque segment commuté.

Vous pouvez choisir l'une de ces options :

- La valeur par défaut du protocole RSTP (Rapid Spanning Tree Protocol) (également appelé protocole MST [Multiple Spanning Tree])
- Le protocole PVST+ (Per-VLAN Spanning Tree)
- Le protocole RPVST+ (Rapid Per-VLAN Spanning Tree)

CONSEIL Si vous connectez le switch à un switch réseau Cisco, la valeur par défaut type est PVST+ et non RSTP. Pour garantir la compatibilité, l'un des deux switchs doit être modifié.

Seuils de port

Les seuils des ports empêchent toute perturbation du trafic sur un réseau local par une tempête de diffusion, de multidiffusion ou d'envoi individuel sur l'une des interfaces physiques. Les seuils des ports ne s'appliquent pas aux switchs avec firmware allégé.

Une tempête survient sur un réseau local lorsque ce dernier est inondé de paquets entraînant un trafic excessif et dégradant les performances du réseau. Des erreurs dans la mise en œuvre de la pile de protocoles, des erreurs dans les configurations réseau ou des utilisateurs émettant des attaques de déni de service peuvent provoquer une tempête.

Trafic entrant (contrôle des tempêtes)

Les seuils du port entrant (ou suppression du trafic) surveille en permanence les paquets transitant d'une interface vers le bus de commutation et détermine le type du paquet (envoi individuel, multidiffusion ou diffusion générale). Le switch compte le nombre de paquets d'un type spécifique reçu dans un intervalle de temps de 1 seconde et compare la mesure avec un seuil de niveau de suppression prédéfini.

Le seuil du port utilise l'une de ces méthodes pour mesurer l'activité du trafic :

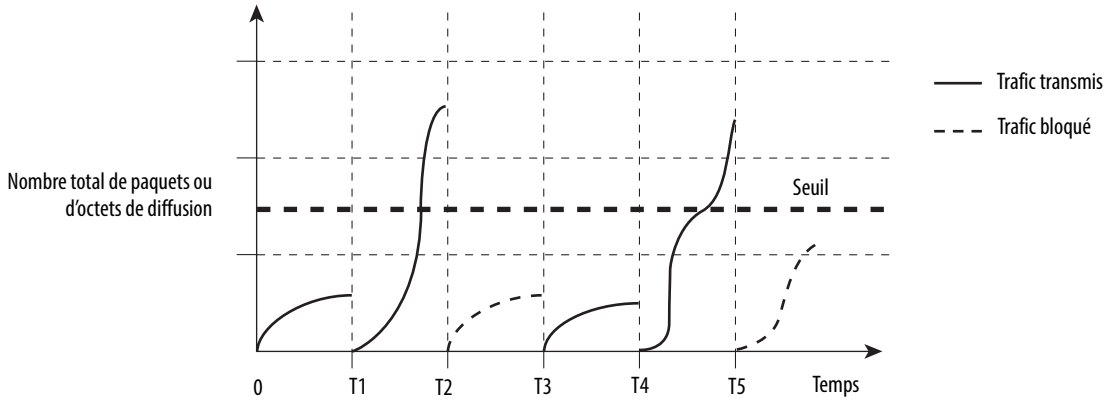
- La bande passante en tant que pourcentage de la bande passante totale disponible du port qui peut être utilisée par le trafic de diffusion générale, de multidiffusion ou d'envoi individuel.
- Le débit du trafic en paquets par seconde (débit de réception des paquets de diffusion, de multidiffusion ou d'envoi individuel).
- Le débit du trafic en bits par seconde (débit de réception des paquets de diffusion générale, de multidiffusion ou d'envoi individuel).

Avec chaque méthode, le port bloque le trafic lorsque le seuil maximal est atteint. Le port reste bloqué jusqu'à ce que le débit du trafic descende sous le seuil, puis reprend un transfert normal. En général, plus le niveau est élevé, moins la protection contre les tempêtes de diffusion est efficace.

IMPORTANT Lorsque le seuil du port en matière de trafic de multidiffusion est atteint, tout le trafic de multidiffusion sauf le trafic de gestion du réseau, comme les trames BDPU et CDP (Cisco Discovery Protocol), est bloqué.

Le graphique présente des modèles de trafic de diffusion générale sur une interface pendant une période de temps donnée. L'exemple peut également être appliqué au trafic de multidiffusion et d'envoi individuel. Dans cet exemple, le trafic de diffusion générale transmis a dépassé le seuil configuré entre les intervalles de temps T1 et T2 et entre les intervalles de temps T4 et T5. Lorsque la quantité de trafic spécifié est supérieure au seuil, tout le trafic correspondant chute pendant la période de temps suivante. Par conséquent, le trafic de diffusion générale est bloqué pendant les intervalles T2 et T5 suivants. Lors de l'intervalle de temps suivant (par exemple, T3), si le trafic de diffusion générale ne dépasse pas le seuil, le transfert reprend.

Figure 2 - Exemple de seuils des ports



La combinaison du niveau de suppression du contrôle des tempêtes et de l'intervalle de temps de 1 seconde contrôle la façon dont fonctionne l'algorithme de seuils des ports. Un seuil plus élevé permet le transfert de davantage de paquets. Une valeur de seuil de 100 % signifie qu'aucune limite n'est imposée au trafic. Une valeur de 0,0 signifie que tout le trafic de diffusion générale, de multidiffusion ou d'envoi individuel sur ce port est bloqué.

IMPORTANT	Parce que les paquets n'arrivent pas à intervalles réguliers, l'intervalle de 1 seconde pendant lequel l'activité du trafic est mesurée peut affecter le comportement des seuils des ports.

Trafic sortant (limitation du débit)

Les seuils des ports sortants limitent le débit de communication du switch avec un dispositif client sous la forme d'un pourcentage de vitesse du câble (quantité de limitation du débit en tant que pourcentage du total). Limiter la bande passante aux utilisateurs et ports spécifiques permet de faciliter le contrôle de la congestion du réseau, d'offrir de meilleures performances, de créer des réseaux efficaces et d'empêcher un petit nombre de dispositifs de monopoliser la bande passante du réseau. Ceci permet également d'améliorer la fiabilité en limitant la bande passante maximale des dispositifs finaux qui ne sont pas capables de prendre en charge de grandes quantités de trafic. Depuis l'interface Internet de Device Manager ou l'application AOP Logix Designer, vous pouvez activer ou désactiver la limitation du débit par port.

Configuration des seuils des ports par défaut

Par défaut, les seuils entrants d'envoi individuel, de diffusion générale et de multidiffusion des ports sont désactivés. Les seuils sortants des ports sont également désactivés.

Sécurité des ports

Les switchs Stratix 5700 implémentent la sécurité des ports en fonction de l'adresse MAC. Une adresse MAC est une adresse unique attribuée à chaque dispositif Ethernet. Cela signifie que le switch peut appliquer des communications de manière statique ou dynamique par adresse MAC.

Avec une sécurité de port dynamique, un port de switch communique avec un certain nombre de dispositifs (adresses MAC). Le port suit uniquement le nombre de dispositifs et non les adresses MAC de ces dispositifs. Dans le cadre d'une sécurité de port statique, les dispositifs sont ajoutés à la table de sécurité des ports à partir de leur adresse MAC. Avec une sécurité de port dynamique et statique, seuls les dispositifs dont l'adresse MAC figure dans la table de sécurité sont en mesure de communiquer sur ce port.

Vous pouvez utiliser une seule de ces méthodes ou les deux sur les switchs Stratix 5700 avec firmware complet au niveau de chaque port. La sécurité des ports ne s'applique pas aux switchs avec firmware allégé.

Adresse MAC sécurisée dynamique (MAC ID)

De nombreux rôles de smartport ont un nombre maximum de MAC 'ID pouvant utiliser ce port. Par exemple, le rôle de smartport « Dispositif d'automatisation » configure le port pour un seul MAC ID. Le MAC ID est dynamique, ce qui signifie que le switch mémorise le MAC ID de la première source à utiliser le port. Les tentatives d'accès au port par toute autre MAC ID sont refusées.

Si la liaison est désactivée, le switch mémorise de nouveau de manière dynamique le MAC ID à protéger.

Le nombre par défaut de MAC ID peut être changé sous l'onglet Port Security dans l'interface Internet de Device Manager ou l'application Logix Designer.

Le tableau ci-dessous montre le rôle de smartport et le nombre maximum de MAC ID pris en charge.

Tableau 5 - Nombre maximum de MAC ID par rôle de smartport

Rôle de smartport	Nombre max de MAC ID
Automation Device	1
Desktop for Automation	1
Switch for Automation	Illimité
Router for Automation	Illimité
Phone for Automation	3
Wireless for Automation	Illimité
Multiport Automation Devices	Illimité
Virtual Desktop for Automation	2
Port Mirroring	Illimité
None	Illimité

Adresse MAC sécurisée statique (MAC ID)

L'autre méthode de limitation des MAC ID consiste à configurer de manière statique un ou plusieurs MAC ID pour un port en les définissant via la sécurité des ports sur l'interface Internet de Device Manager. Ces adresses font ainsi partie de la configuration enregistrée du switch. Cette méthode fournit une excellente sécurité. Toutefois, si vous remplacez les dispositifs connectés au port, vous devez reconfigurer les MAC ID, car les nouveaux dispositifs ont un MAC ID différent de celui des dispositifs précédents.

Violations de sécurité

Il y a violation de la sécurité lorsque l'une des situations suivantes se produit :

- Le nombre maximal d'adresses MAC sécurisées qui ont été configurées pour un port a été ajouté à la table des adresses et une station dont l'adresse MAC ne figure pas dans la table des adresses tente d'accéder à l'interface.
- Une adresse mémorisée ou configurée sur une interface sécurisée est visible sur une autre interface sécurisée dans le même VLAN.

Lorsqu'une violation se produit, le port bascule en mode de restriction. Dans ce mode, les paquets dont l'adresse source est inconnue sont supprimés et vous êtes averti qu'une violation de la sécurité s'est produite. Une interruption SNMP est envoyée, un message syslog est consigné et le compteur de violation est incrémenté.

EtherChannels

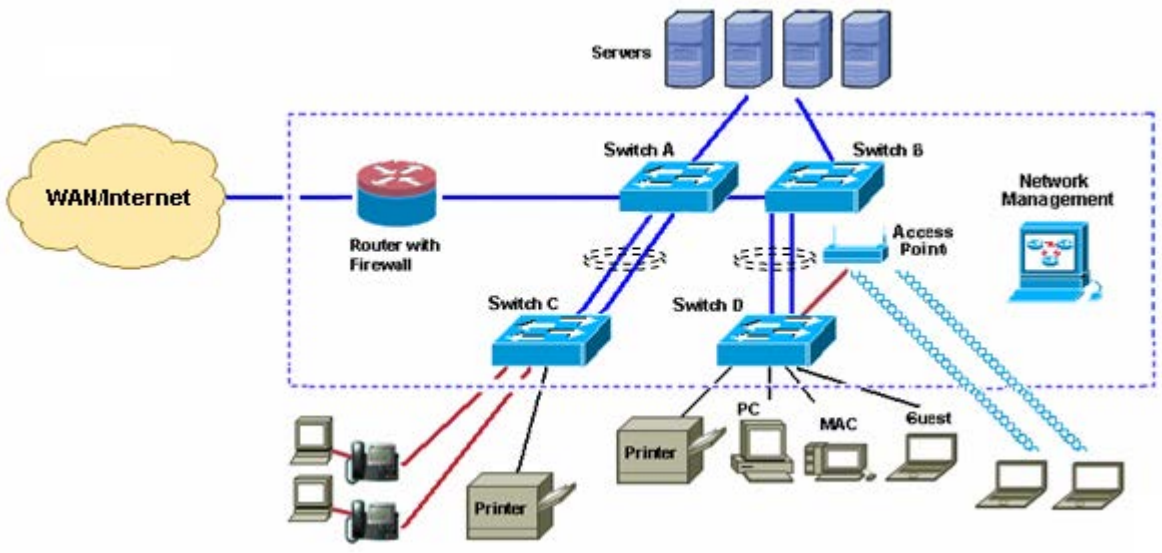
Un EtherChannel (ou groupe de ports) est un groupe d'au moins deux ports de switch Fast Ethernet ou Gigabit Ethernet regroupés en une seule liaison logique, créant ainsi une liaison de bande passante plus importante entre deux switchs.

Le switch prend en charge jusqu'à six EtherChannels. Chaque EtherChannel peut comprendre jusqu'à huit ports Ethernet compatibles et configurés.
Les EtherChannels ne s'appliquent pas aux switchs avec firmware allégé.

La figure suivante montre deux EtherChannels. Deux ports full-duplex de 10/100/1000 Mbits/s sur les switchs A et C créent un EtherChannel avec une bande passante pouvant atteindre 4 Gbits/s entre les deux switchs. De même, deux ports full-duplex de 10/100 Mbits/s sur les switchs B et D créent un EtherChannel avec une bande passante pouvant atteindre 400 Mbits/s entre les deux switchs.

En cas d'indisponibilité de l'un des ports de l'EtherChannel, le trafic est envoyé via les ports restants au sein de l'EtherChannel.

Figure 3 - Exemple d'EtherChannel



Vous pouvez configurer un EtherChannel dans l'un de ces modes :

- Port Aggregation Protocol (PAgP)
- Link Aggregation Control Protocol (LACP)
- On

Configurez les deux extrémités de l'EtherChannel dans le même mode :

- Lorsque vous configurez une extrémité d'un EtherChannel en mode PAgP ou LACP, le système négocie avec l'autre extrémité de la voie afin de déterminer les ports à activer. Les ports incompatibles sont arrêtés. Au lieu d'être arrêté, le port local devient indépendant et continue de transmettre le trafic de données comme toutes les autres liaisons uniques. La configuration du port ne change pas, mais le port ne participe pas à l'EtherChannel.

- Lorsque vous configurez un EtherChannel en mode activé, aucune négociation n'a lieu. Le switch force l'activation de tous les ports compatibles sur l'EtherChannel. L'autre extrémité de la voie (sur l'autre switch) doit également être configurée sur le mode de fonctionnement activé. Dans le cas contraire, une perte de paquets peut se produire.

Si une liaison d'un EtherChannel échoue, le trafic acheminé précédemment via la liaison défaillante bascule vers les liaisons restantes au sein de l'EtherChannel. Si les interruptions sont activées sur la switch, une interruption pour cause de défaillance est envoyée ; elle identifie le switch, l'EtherChannel et la liaison défaillante. Les paquets entrants de diffusion générale et de multidiffusion d'une seule liaison sur un EtherChannel sont bloqués et ne peuvent pas revenir sur une autre liaison de l'EtherChannel.

Persistance DHCP

Chaque dispositif d'un réseau IP doit avoir une adresse IP unique. Le protocole DHCP (Dynamic Host Configuration Protocol) attribue automatiquement des informations d'adresse IP à partir d'un ensemble d'adresses disponibles pour les dispositifs nouvellement connectés (les clients DHCP) au réseau. Si un dispositif est déconnecté, puis reconnecté au réseau, il reçoit l'adresse IP disponible suivante, qui peut être la même adresse que celle qu'il avait précédemment ou une autre.

Le switch peut être configuré pour fonctionner comme un serveur DHCP pour fournir la persistance DHCP. Avec la persistance DHCP, vous pouvez affecter une adresse IP spécifique à chaque port pour vous assurer qu'un dispositif connecté à un port spécifique reçoit la même adresse IP. Cette caractéristique fonctionne uniquement si un seul dispositif est connecté à chaque port configuré pour la persistance DHCP.

IMPORTANT Pour vous assurer que la persistance DHCP fonctionne correctement, suivez les règles d'application.

Synchronisation du temps CIP Sync (protocole PTP)

La norme IEEE 1588 définit le protocole PTP (Precision Time Protocol) qui permet une synchronisation précise des horloges des systèmes de mesure et de commande. Nous appelons cette caractéristique la synchronisation temporelle CIP. Les horloges sont synchronisées sur le réseau de communication EtherNet/IP. Le protocole PTP permet de synchroniser les horloges des systèmes dont la précision, la résolution et la stabilité diffèrent. Le protocole PTP génère une relation maître-esclave parmi les horloges du système. En définitive, toutes les horloges s'alignent sur l'heure d'une horloge sélectionnée comme étant l'horloge principale.

Trois modes de protocole PTP sont disponibles pour les switchs :

- Boundary Clock
- Transparent Clock
- Forwarding (le protocole PTP est désactivé lorsque le mode Forwarding est sélectionné)

Pour plus d'informations sur ces modes, reportez-vous à la publication ENET-TD001, Converged Plantwide Ethernet Design and Implementation.

Le mode PTP par défaut est le mode Forwarding.

Service NAT (Network Address Translation)

Le service NAT convertit une adresse IP en une autre adresse IP via un switch configuré pour-NAT. Le switch convertit les adresses source et de destination au sein des paquets de données lorsque le trafic parcourt les sous réseaux.

Ce service est utile si vous avez besoin de réutiliser les adresses IP sur un réseau. Par exemple, NAT permet aux dispositifs qui partagent une seule adresse IP sur un sous-réseau privé de segmenter ce dernier en plusieurs sous-réseaux privés identiques tout en conservant des identités uniques sur le sous-réseau public.(1)

La mise en œuvre du service NAT sur le switch Stratix 5700 est spécifique :

- NAT un à un — le switch utilise le service NAT un à un, plutôt qu'un service un-à-plusieurs. Le service NAT un-à-un requiert que chaque adresse source soit convertie en une adresse de destination unique. Contrairement au service NAT un-à-plusieurs, plusieurs adresses source ne peuvent pas partager la même adresse de destination.
- Mise en œuvre de la couche 2 — la mise en œuvre du service NAT du switch fonctionne au niveau de la couche 2 (MAC). À ce niveau, le switch ne peut remplacer que les adresses IP et n'agit pas comme un routeur.

Présentation de la configuration

Pour configurer le service NAT, vous créez une ou plusieurs instances NAT uniques. Dans une implémentation type, une seule instance est nécessaire. Une instance NAT contient des entrées qui définissent chaque conversion d'adresse, ainsi que d'autres paramètres de configuration.

Les conversions que vous définissez dépendent de la façon dont le trafic est acheminé - via un switch de couche 3, un routeur ou un switch de couche 2 :

- Si le trafic est acheminé via un switch de couche 3 ou un routeur (Figure 4), vous devez définir :
  - Une conversion privé-public pour chaque dispositif sur le sous-réseau privé qui doit communiquer sur le sous-réseau public.
  - Une conversion de passerelle pour le switch de couche 3 ou le routeur.

  Vous n'avez pas besoin de configurer le service NAT pour tous les dispositifs sur le sous-réseau privé. Par exemple, vous pouvez choisir d'omettre certains dispositifs du service NAT pour accroître la sécurité, réduire le trafic ou conserver un espace d'adresse public.

  IMPORTANT Nous vous recommandons comme bonne pratique d'acheminer le trafic via un switch de couche 3 ou un routeur.

- Si le trafic est acheminé via un switch de couche 2 (Figure 5), vous devez définir :
  - Une conversion privé-public pour chaque dispositif sur le sous-réseau privé qui doit communiquer sur le sous-réseau public.
  - Une conversion public-privé pour chaque dispositif sur le sous-réseau public qui doit communiquer sur le sous-réseau privé.

(1) Notez que nous avons utilisé les termes public et privé pour différencier les deux réseaux de chaque côté du dispositif NAT. Cela ne signifie pas que le réseau public doit être acheminable via Internet.

Figure 4 - Exemple de couche 3

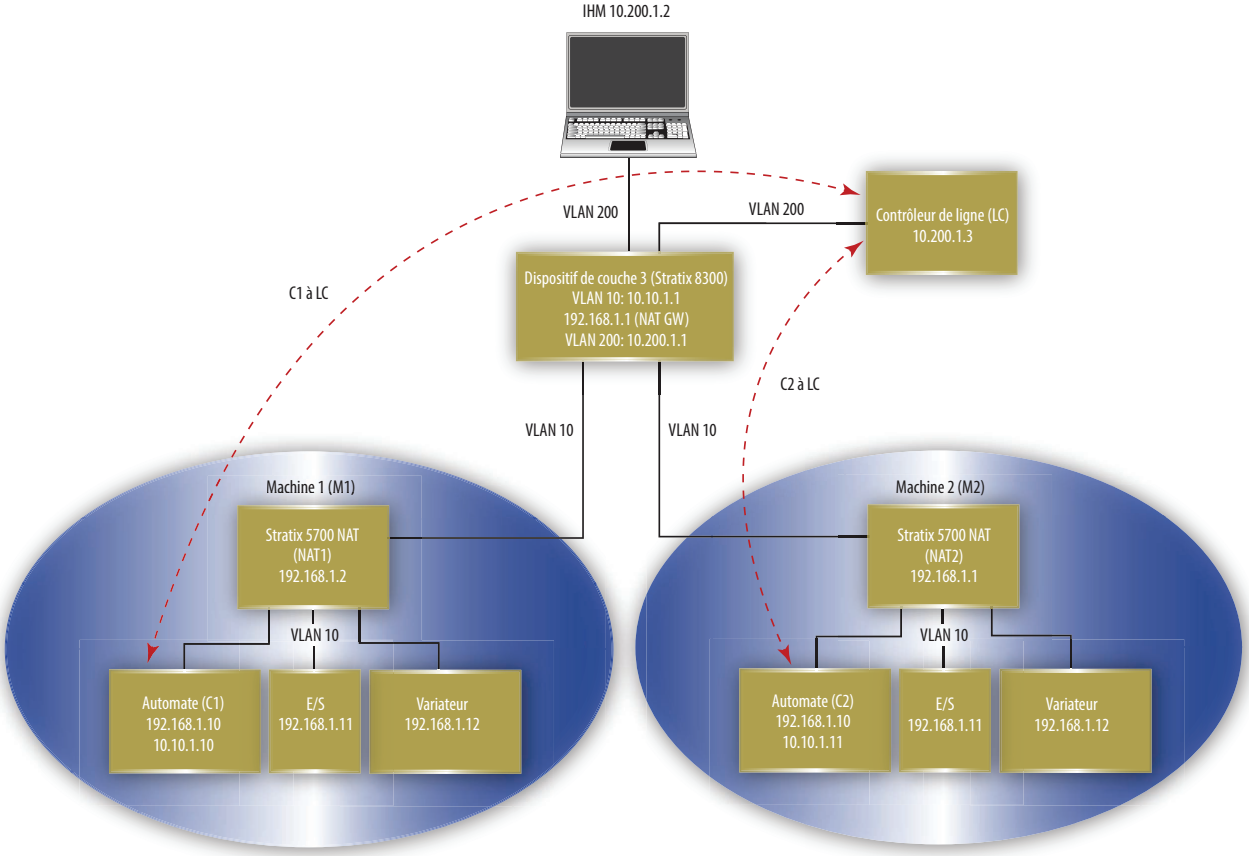
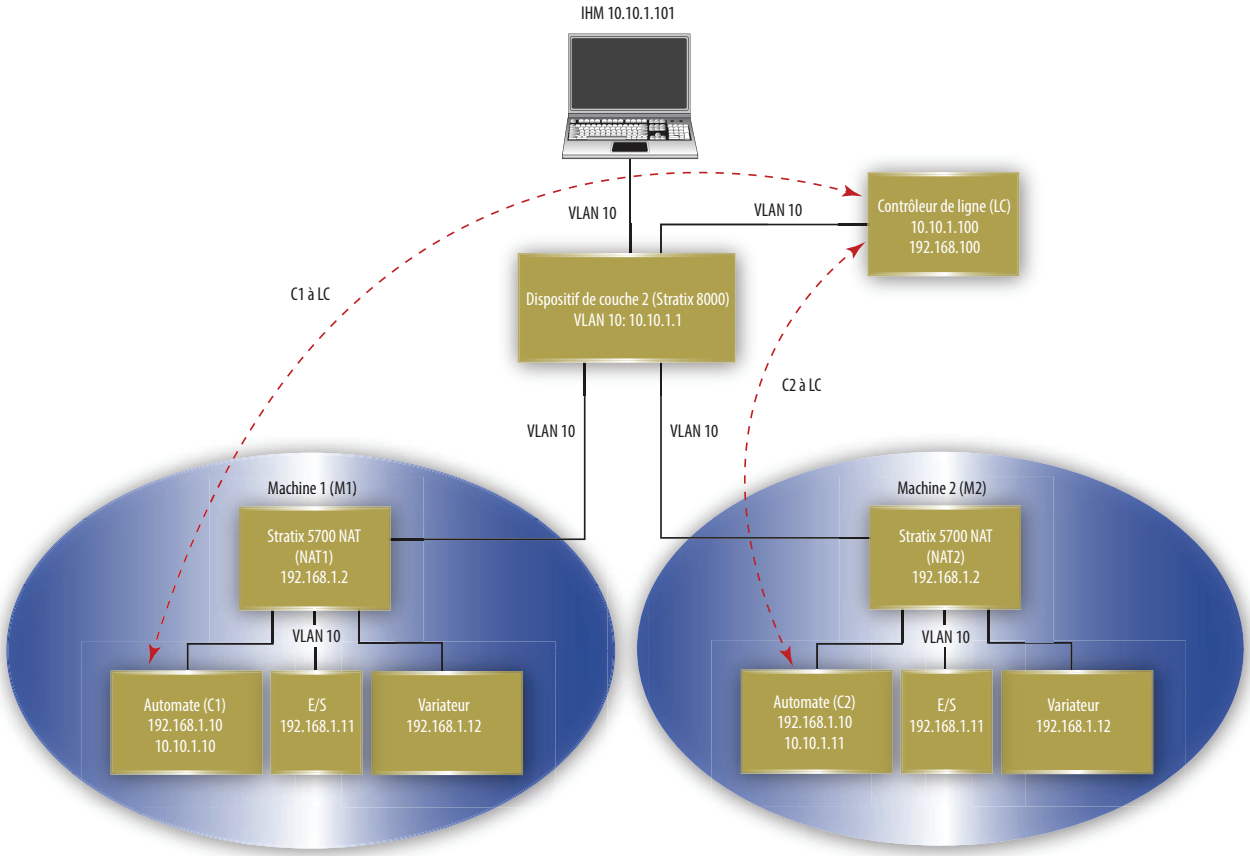


Figure 5 - Exemple de couche 2



Il existe trois types de conversion d'adresse. Le type de conversion détermine le nombre d'entrées de conversion. Un switch peut compter un maximum de 128 entrées de conversion.

Tableau 6 - Nombre d'entrées de conversion par type de conversion

Type de conversion	Entrées de conversion	Description
Single	1	Convertit une seule adresse IP. Comprend les éléments suivants : • Une adresse IP privée • Une adresse IP publique
Range	Plusieurs	Convertit une plage d'adresses IP. Comprend les éléments suivants : • Une adresse IP privée de départ • Une adresse IP publique de départ • Plusieurs entrées en fonction de la plage spécifiée
Subnet	1	Convertit toutes les adresses IP au sein d'un sous-réseau ou d'une partie d'un sous-réseau. Comprend les éléments suivants : • Une adresse IP privée de départ • Une adresse IP publique de départ alignée sur les limites du sous-réseau valide • Un masque de sous-réseau

EXEMPLE Les types suivants de conversion comptent comme 10 entrées de conversion :

- Conversion unique pour un seul dispositif
- Plage de conversion pour huit dispositifs
- Conversion du sous-réseau pour tous les dispositifs sur le sous-réseau

Les types de conversion de plage et unique ont une relation de type un à un entre les entrées de conversion et les adresses à convertir. Cependant, les conversions de sous-réseau ont une relation de type un à plusieurs autorisant une entrée de conversion pour plusieurs adresses.

Affectations de VLAN

Lors de la configuration du service NAT, vous pouvez assigner un ou plusieurs VLAN à une instance NAT. Lorsque vous assignez un VLAN à une instance NAT, le trafic associé à ce VLAN est soumis aux paramètres de configuration de l'instance NAT. Les paramètres de configuration indiquent si le trafic est converti, corrigé, bloqué ou de transit.

IMPORTANT Configurez tous les rôles de smartport et les VLAN avant de créer des instances NAT.

Si vous modifiez un rôle de smartport ou le VLAN natif pour un port associé à une instance NAT, vous devez réaffecter les VLAN à l'instance NAT.

Lorsque vous assignez des VLAN à une instance NAT, considérez les points suivants :

- NAT prend en charge les ports trunk et les ports d'accès.
- NAT ne modifie pas les points du VLAN.
- Vous pouvez assigner jusqu'à 128 VLAN maximum à une ou plusieurs instances.

- Vous pouvez assigner le même VLAN à plusieurs instances tant que le VLAN est associé à des ports différents. Par exemple, vous pouvez assigner le VLAN 1 aux instances A et B tant que le VLAN 1 est associé au port Gi1/1 sur l'instance A et au port Gi1/2 sur l'instance B.
- Par défaut, chaque instance est affectée à tous les VLAN sur le port Gi1/1 et à aucune instance sur le port Gi1/2.

Les VLAN associés à un port trunk peuvent être assignés ou non à une instance NAT :

- Si un VLAN est assigné à une instance NAT, son trafic est soumis aux paramètres de configuration de l'instance NAT.
- Si un VLAN n'est pas assigné à une instance NAT, son trafic n'est pas converti et est toujours autorisé à transiter par le port trunk.

Interface de gestion et VLAN

L'interface de gestion peut être associée à un VLAN assigné ou non à une instance NAT :

- Si le VLAN associé est assigné à une instance NAT, l'interface de gestion réside sur le sous-réseau privé par défaut. Pour gérer le switch du sous-réseau privé, aucune configuration supplémentaire n'est nécessaire. Pour gérer le switch du sous-réseau public, vous devez configurer une conversion privé-public.
- Si le VLAN associé n'est pas assigné à une instance NAT, le trafic de l'interface de gestion n'est pas converti et est toujours autorisé à transiter par le port trunk.

Considérations relatives à la configuration

Tenez compte des lignes directrices et des limites suivantes lors de la configuration du service NAT :

- Un switch ne peut convertir que les adresses IPv4.
- Un switch peut prendre une charge jusqu'à 128 instances NAT, 128 -VLAN associés au service NAT et 128 entrées de conversion. Une conversion de sous-réseau compte comme une seule entrée de conversion, mais comprend des conversions pour de nombreux dispositifs.
- Vous pouvez configurer le service NAT sur un ou les deux ports de liaison montante du switch.

IMPORTANT	Certaines configurations NAT peuvent entraîner une hausse des charges de trafic plus importantes que prévu sur les sous-réseaux privé et public. En outre, le trafic fortuit peut être visible. Le service NAT ne remplace pas un pare-feu. Assurez-vous que votre configuration offre les performances appropriées avant de l'utiliser dans un environnement de production.

Les ports configurés pour le service NAT **ne prennent pas en charge** les éléments suivants au-delà de la limite NAT en raison des adresses IP intégrées non corrigées, des adresses IP chiffrées ou de la dépendance vis-à-vis du trafic de multidiffusion :

- Chiffrement du trafic et protocoles de vérification de l'intégrité généralement incompatibles avec le service NAT, y compris le mode de transport IPsec (module 1756-EN2TSC)
- Applications qui utilisent des initiations de session dynamiques, comme NetMeeting
- Protocole FTP (File Transfer Protocol)
- Le modèle DCOM (Microsoft Distributed Component Object Model), qui est utilisé dans les communications OPC (Open Platform Communications)
- Le trafic de multidiffusion, y compris les applications qui utilisent la multidiffusion, comme CIP Sync (IEEE1588) et la redondance CLX

Autorisations et corrections du trafic

Tandis qu'un port configuré pour le service NAT peut convertir de nombreux types de trafic, seul le trafic d'envoi individuel et de diffusion générale est pris en charge. Vous pouvez choisir de bloquer ou transférer les types de trafic suivants qui ne sont pas gérés par le service NAT :

- Trafic d'envoi individuel non converti
- Trafic de multidiffusion
- Trafic IGMP

Par défaut, tous les types de trafic ci-dessus sont bloqués.

Certains types de trafic doivent être corrigés pour fonctionner correctement avec le service NAT, car les paquets intègrent des adresses IP. Le switch prend en charge les corrections pour les types de trafic suivants :

- Protocole ARP (Address Resolution Protocol)
- Protocole ICMP (Internet Control Message Protocol)

Par défaut, les corrections sont activées pour les protocoles ARP et ICMP.

Protocole REP (Resilient Ethernet Protocol)

Le protocole REP (Resilient Ethernet Protocol) offre une alternative au protocole STP (Spanning Tree Protocol) pour contrôler les anneaux et les boucles du réseau, gérer les défaillances de liaison et améliorer le temps de convergence. Le protocole REP contrôle un groupe de ports connectés dans un segment, s'assure que le segment ne crée pas de boucles de pontage répond aux défaillances de liaison au sein du segment. Le protocole REP fournit une base d'élaboration de réseaux plus complexes et prend en charge l'équilibrage de charge du VLAN.

Le protocole REP est un protocole de segment. Un segment REP est une chaîne de ports connectés entre eux et configurés avec un ID de segment. Chaque segment se compose de ports de segment (transit) standard et de deux ports frontaux configurés par l'utilisateur. Un switch ne peut pas avoir plus de deux ports appartenant au même segment et chaque port de segment ne peut avoir qu'un seul voisin externe. Un segment peut transiter par un support partagé, mais sur une liaison, seuls deux ports peuvent appartenir au même segment. Le protocole REP est pris en charge uniquement sur les interfaces trunk de couche 2. La sélection du switch pour le smartport d'automatisation valide le partage de couche 2. Le protocole REP est pris en charge sur les EtherChannels, mais pas sur un port individuel appartenant à un EtherChannel.

Vous pouvez construire presque tout type de réseau à partir de segments REP. Le protocole REP prend également en charge l'équilibrage de la charge du VLAN. Ce dernier est contrôlé par le port frontal principal, mais se produit sur n'importe quel port du segment.

Ces types de ports REP sont sélectionnables dans l'interface Internet de Device Manager :

- Primary - ce port est un port frontal principal. Ce port participe toujours à l'équilibrage de la charge du VLAN dans le segment REP.
- Edge - ce port est un port frontal secondaire. Ce port participe également à l'équilibrage de la charge du VLAN dans le segment REP.

  Les ports frontaux sont des points de terminaison d'un segment REP. L'utilisateur doit configurer deux ports frontaux, y compris un port frontal principal, pour chaque segment REP. Entrer « edge » sans port frontal principal configure automatiquement le port en tant que port frontal secondaire. Les ports frontaux principal et secondaire doivent être configurés même si la prise en charge de l'équilibrage du VLAN n'est pas nécessaire.
- Transit - ce port n'est pas un port frontal dans le segment REP.
- No-Neighbor Primary - ce port est un port frontal principal connecté à un switch non REP.
- No-Neighbor - ce port est un port frontal secondaire connecté à un switch non REP.

  Les ports frontaux « no-neighbor » (sans voisin) intègrent toutes les propriétés des ports frontaux standard. Ces ports permettent la construction d'un anneau REP contenant un switch qui ne prend pas en charge le protocole REP.
- None - ce port n'appartient pas au segment REP.

Les protocoles REP et STP peuvent coexister sur le même switch, mais pas sur le même port. Le protocole REP n'interagit pas avec le protocole STP. Par exemple, si un port est configuré comme un port REP, le protocole STP est désactivé sur ce port. Les BPDU ne sont ni acceptées ni envoyées aux ports REP. Cependant, les anneaux ou domaines REP et STP adjacents peuvent partager une liaison commune. Cette liaison commune peut être utilisée pour transférer le trafic de plan de date REP et STP ou pour le trafic de plan de contrôle STP.

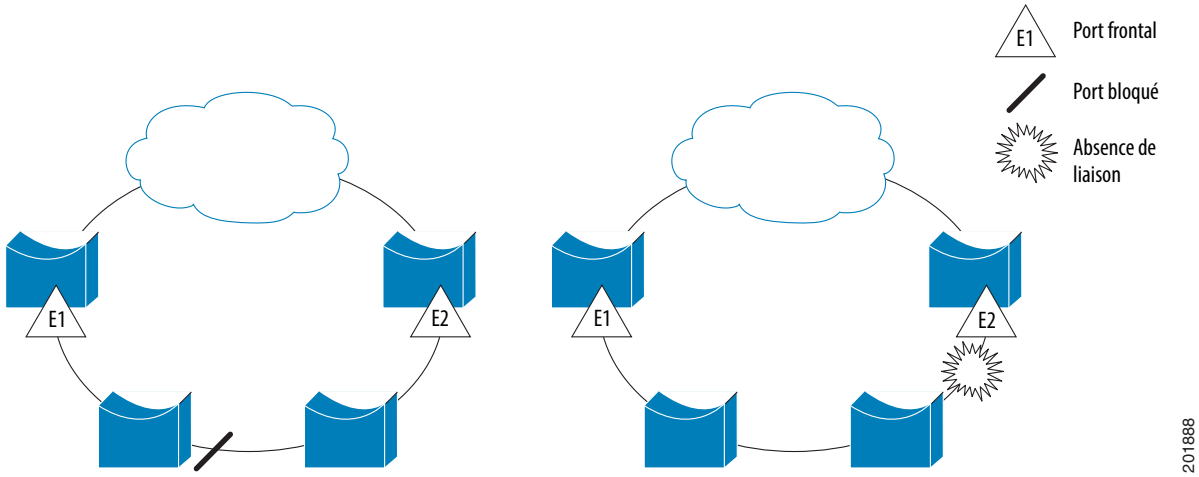
La Figure 6 montre un exemple de segment composé de six ports répartis sur quatre switchs. Les ports E1 et E2 sont configurés en tant que ports frontaux. Lorsque tous les ports sont opérationnels (comme sur le segment de gauche), un seul port est bloqué, représenté par la ligne en diagonale. Lorsqu'il y a une défaillance sur le réseau, comme illustré sur le schéma de droite, le port bloqué revient à l'état de transfert pour minimiser la perturbation du réseau.

Segment ouvert REP

Le segment illustré sur la Figure 6 est un segment ouvert. Il n'y a pas de connectivité entre les deux ports frontaux. Le segment REP ne peut pas produire de boucle de raccordement. Vous pouvez raccorder en toute sécurité les ports frontaux du segment à un réseau. Tous les hôtes raccordés aux switchs dans le segment peuvent se connecter de deux manières au reste du réseau via les ports frontaux, mais seule une connexion est accessible à tout temps. Si suite à une défaillance, un hôte ne peut pas accéder à sa passerelle habituelle, le protocole REP débloque tous les ports pour s'assurer que la connectivité est disponible par l'intermédiaire de l'autre passerelle.

Dans l'exemple suivant, E1 ou E2 peut être configuré en tant que port frontal principal.

Figure 6 - Exemple de segment ouvert

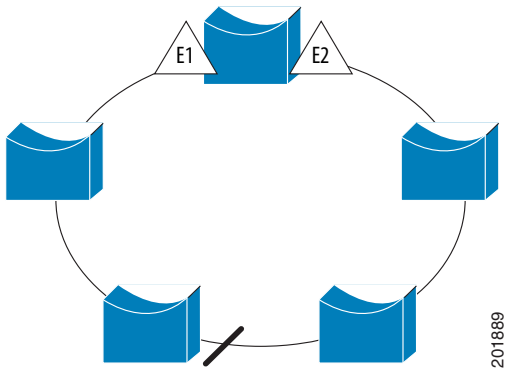


Segment annulaire REP

Le segment illustré sur la Figure 7, avec les deux ports frontaux sur le même switch, est un segment annulaire. Dans cette configuration, la connectivité entre les ports frontaux est assurée via le segment. Avec cette configuration, vous pouvez créer une connexion redondante entre deux switchs du segment.

Sur la figure suivante, E1 ou E2 peut être configuré en tant que port frontal principal.

Figure 7 - Exemple de segment annulaire



Les segments REP ont les caractéristiques suivantes :

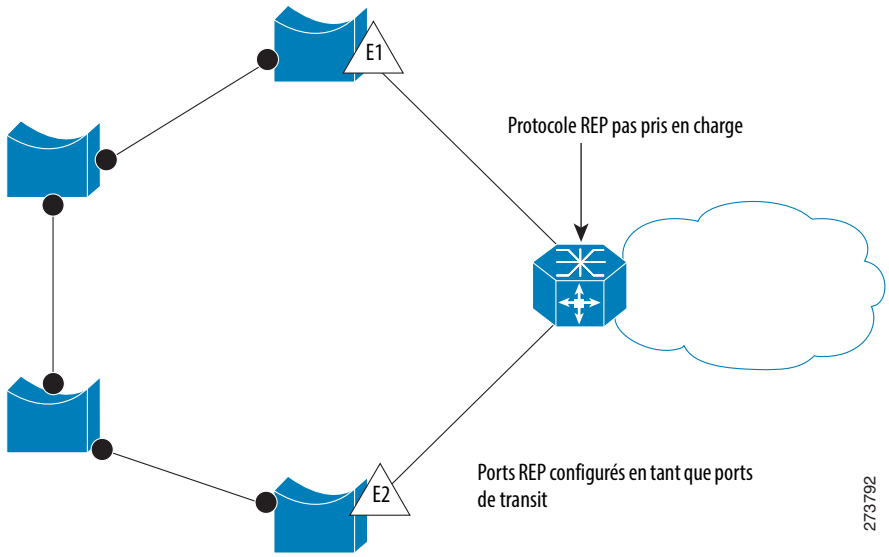
- Si tous les ports du segment sont opérationnels, un port (dénommé le port de rechange) est bloqué pour chaque VLAN.
- Si l'équilibrage de la charge des VLAN est configuré, deux ports du segment contrôlent l'état bloqué des VLAN.
- Si un ou plusieurs ports d'un segment ne sont pas opérationnels, provoquant ainsi une défaillance de la liaison, tous les ports transfèrent le trafic de tous les VLAN pour prendre en charge la connectivité continue.
- Dans le cas d'une défaillance de la liaison, les ports de rechange sont débloqués aussi rapidement que possible. Lorsque la liaison défaillante est restaurée, un port logiquement bloqué par VLAN est sélectionné avec une perturbation minimale du réseau.

Topologies d'accès en anneau

Dans les topologies d'accès en anneau, le switch voisin ne peut pas prendre en charge le protocole REP, comme illustré sur la Figure 8. Dans ce cas, vous pouvez configurer les ports frontaux non REP (E1 et E2) en tant que ports frontaux sans voisin. Ces ports héritent de toutes les propriétés des ports frontaux et vous pouvez les configurer comme n'importe quel port frontal, y compris pour envoyer des avis de modification de la topologie STP ou REP au switch d'agrégation. Dans ce cas, l'avis de modification de la topologie STP (TCN) qui est envoyé est un message STP MST (multiple spanning-tree – arbre maximal multiple).

Dans l'exemple suivant, E1 ou E2 peut être configuré en tant que port principal sans voisin.

Figure 8 - Exemple de topologie en anneau



Limitations du protocole REP :

- Vous devez configurer chaque port du segment. Une configuration incorrecte peut provoquer des boucles de transfert dans les réseaux.
- Le protocole REP peut gérer uniquement un seul port défaillant au sein du segment. Plusieurs ports défaillants au sein du segment REP entraînent une perte de connectivité réseau.

Configurez le protocole REP uniquement dans les réseaux avec redondance. Configurer le protocole REP dans un réseau sans redondance provoque une perte de connectivité.

Intégrité des liaisons

Le protocole REP n'utilise pas de mécanisme d'interrogation de bout en bout entre les ports finaux pour vérifier l'intégrité de la liaison. Il implémente la détection de défaillance de la liaison locale. La couche LSL (Link Status Layer) du protocole REP détecte son voisin compatible REP et établit une connectivité au sein du segment. Tous les VLAN sont bloqués sur une interface jusqu'à la détection du voisin. Une fois le voisin identifié, le protocole REP détermine le port voisin à basculer en port de rechange et les ports de transfert du trafic.

Chaque port d'un segment possède un ID de port unique. Le format de l'ID de port est similaire à celui utilisé par l'algorithme de l'arbre maximal: un numéro de port (unique sur le pont), associé à une adresse MAC (unique sur le réseau). Lorsqu'un port de segment est entrant, sa LSL commence à envoyer des paquets qui incluent l'ID du segment et l'ID du port. Le port est déclaré comme étant opérationnel après avoir effectué une négociation tridirectionnelle avec un voisin sur le même segment.

SNMP

Le switch prend en charge les versions 1, 2C et 3 du protocole SNMP (Simple Network Management Protocol). Le protocole SNMP permet de gérer le switch à distance grâce à d'autres logiciels de gestion du réseau. Cette fonctionnalité est désactivée par défaut.

Le protocole SNMP repose sur trois concepts :

- Gestionnaires SNMP (logiciel client)
- Agents SNMP (dispositifs réseau)
- Base de données de gestion MIB (Management Information Base)

Reportez-vous à MIB prises en charge, à la page 91 pour en savoir plus sur les MIB prises en charge par le switch.

Le gestionnaire SNMP exécute le logiciel de gestion SNMP. Les dispositifs réseau à gérer, comme les ponts, les routeurs, les serveurs et les stations de travail, ont un module de logiciel agent. L'agent fournit un accès à une MIB locale d'objets qui reflètent les ressources et l'activité du dispositif. L'agent répond également aux commandes du gestionnaire pour récupérer les valeurs de la MIB et définir des valeurs dans la MIB. L'agent et la MIB sont sur le switch. Pour configurer le protocole SNMP sur le switch, vous définissez la relation entre le gestionnaire et l'agent.

SNMPv1 et v2C utilisent une forme de sécurité reposant sur la communauté. Les gestionnaires SNMP peuvent accéder à la MIB de l'agent grâce à des mots de passe correspondant aux chaînes de la communauté. SNMPv1 et v2C sont généralement utilisés pour la surveillance du réseau sans contrôle réseau.

SNMPv3 assure la surveillance et le contrôle du réseau. Il fournit un accès sécurisé aux dispositifs par une combinaison d'authentification et de chiffrement des paquets sur le réseau. Le modèle de sécurité utilisé par le protocole SNMPv3 est une stratégie d'authentification configurée pour un utilisateur et son groupe. Un niveau de sécurité correspond au niveau de sécurité autorisée dans un modèle de sécurité. Une combinaison d'un modèle de sécurité et d'un niveau de sécurité détermine le mécanisme de sécurité utilisé pour un paquet SNMP.

Voici quelques directives sur les objets SNMPv3 :

IMPORTANT SNMPv.3 est disponible uniquement dans la version cryptographique du firmware du switch.

- Chaque utilisateur appartient à un groupe.
- Un groupe définit la stratégie d'accès d'un ensemble d'utilisateurs.
- Une politique d'accès définit les objets SNMP accessibles en lecture, écriture et création.
- Un groupe détermine la liste des notifications que ses utilisateurs peuvent recevoir.
- Un groupe définit également le modèle de sécurité et le niveau de sécurité de ses utilisateurs.
- Une vue SNMP est une liste de MIB à laquelle un groupe peut accéder.
- Il est possible de collecter les données en toute sécurité depuis les dispositifs SNMP sans crainte qu'elles soient trafiquées ou corrompues.
- Des informations confidentielles, par exemple, les paquets de commandes SNMP Set qui modifient une configuration de routeur peuvent être chiffrés pour empêcher le contenu d'être exposé sur le réseau.

MIB prises en charge

Le switch Stratix 5700 prend en charge les MIB suivantes.

Tableau 7 - MIB prise en charge

Nom de la MIB		
BRIDGE-MIB	CISCO-MEMORY-POOL-MIB	IP-MIB
CALISTA-DPA-MIB	CISCO-PAE-MIB	LLDP-EXT-MED-MIB
CISCO-ACCESS-ENVMON-MIB	CISCO-PAGP-MIB	LLDP-MIB
CISCO-ADMISSION-POLICY-MIB	CISCO-PING-MIB	NETRANGER
CISCO-AUTH-FRAMEWORK-MIB	CISCO-PORT-QOS-MIB	NOTIFICATION-LOG-MIB
CISCO-BRIDGE-EXT-MIB	CISCO-PORT-SECURITY-MIB	OLD-CISCO-CHASSIS-MIB
CISCO-BULK-FILE-MIB	CISCO-PORT-STORM-CONTROL-MIB	OLD-CISCO-CPU-MIB
CISCO-CABLE-DIAG-MIB	CISCO-PRIVATE-VLAN-MIB	OLD-CISCO-FLASH-MIB
CISCO-CALLHOME-MIB	CISCO-PROCESS-MIB	OLD-CISCO-INTERFACES-MIB
CISCO-CAR-MIB	CISCO-PRODUCTS-MIB	OLD-CISCO-IP-MIB
CISCO-CDP-MIB	CISCO-RESILIENT-ETHERNET-PROTOCOL-MIB	OLD-CISCO-MEMORY-MIB
CISCO-CIRCUIT-INTERFACE-MIB	CISCO-RTTMON-ICMP-MIB	OLD-CISCO-SYS-MIB
CISCO-CLUSTER-MIB	CISCO-RTTMON-IP-EXT-MIB	OLD-CISCO-SYSTEM-MIB
CISCO-CONFIG-COPY-MIB	CISCO-RTTMON-MIB	OLD-CISCO-TCP-MIB
CISCO-CONFIG-MAN-MIB	CISCO-RTTMON-RTP-MIB	OLD-CISCO-TS-MIB
CISCO-DATA-COLLECTION-MIB	CISCO-SNMP-TARGET-EXT-MIB	RMON-MIB
CISCO-DHCP-SNOOPING-MIB	CISCO-STACK-MIB	RMON2-MIB
CISCO-EMBEDDED-EVENT-MGR-MIB	CISCO-STACKMAKER-MIB	SMON-MIB
CISCO-ENTITY-ALARM-MIB	CISCO-STP-EXTENSIONS-MIB	SNMP-COMMUNITY-MIB
CISCO-ENTITY-VENDORTYPE-OID-MIB	CISCO-SYSLOG-MIB	SNMP-FRAMEWORK-MIB
CISCO-ENVMON-MIB	CISCO-TCP-MIB	SNMP-MPD-MIB
CISCO-ERR-DISABLE-MIB	CISCO-UDLDP-MIB	SNMP-NOTIFICATION-MIB
CISCO-FLASH-MIB	CISCO-VLAN-IFTABLE-RELATIONSHIP-MIB	SNMP-PROXY-MIB
CISCO-FTP-CLIENT-MIB	CISCO-VLAN-MEMBERSHIP-MIB	SNMP-TARGET-MIB
CISCO-IF-EXTENSION-MIB	CISCO-VTP-MIB	SNMP-USM-MIB
CISCO-IGMP-FILTER-MIB	ENTITY-MIB	SNMP-VIEW-BASED-ACM-MIB
CISCO-IMAGE-MIB	ETHERLIKE-MIB	SNMPv2-MIB
CISCO-IP-STAT-MIB	HC-RMON-MIB	TCP-MIB
CISCO-LAG-MIB	IEEE8021-PAE-MIB	UDP-MIB
CISCO-LICENSE-MGMT-MIB	IEEE8023-LAG-MIB	
CISCO-MAC-AUTH-BYPASS-MIB	IF-MIB	
CISCO-MAC-NOTIFICATION-MIB	IP-FORWARD-MIB	

Mise en miroir de ports

La mise en miroir de ports est destinée aux utilisateurs avancés ayant une expérience dans le dépannage du trafic et les problèmes de protocole sur les réseaux. La fonction de mise en miroir de ports copie (ou met en miroir) le trafic d'un port sur un port de surveillance où le paquet peut être capturé par un outil d'analyse des protocoles réseau. Utilisez la mise en miroir de ports comme un outil de diagnostic ou une fonctionnalité de débogage.

La mise en miroir de ports n'affecte pas la commutation du trafic réseau sur le port surveillé. Vous devez dédier un port de surveillance pour utiliser la mise en miroir de ports. À l'exception du trafic qui est copié dans le cadre de la session de mise en miroir de ports, le port de surveillance ne reçoit pas ou ne transfère pas le trafic.

Vous pouvez configurer la mise en miroir de ports en assignant le rôle de smartport de mise en miroir de ports à un port du switch via l'interface Internet de Device Manager.

Routage

Le switch prend en charge les formes de routage suivantes :

- Static routin - définit les chemins d'accès explicites entre deux dispositifs (routeurs et switchs). Vous devez définir manuellement les informations de routage, y compris l'adresse IP de la destination, le masque de sous-réseau de la destination et la prochaine adresse IP du routeur de transit.

- Connected routin - permet à tous les dispositifs sur un VLAN qui utilise le switch de communiquer entre eux s'ils utilisent le switch en tant que passerelle par défaut. Le routage connecté est automatiquement activé si vous activez le routage statique. Pour désactiver le routage connecté et empêcher la communication inter-VLAN, vous devez configurer des listes de contrôle d'accès (ACL) à l'aide de l'interface CLI.

L'activation du routage est un processus en deux étapes au sein de l'interface Internet de Device Manager :

1. Réallouez la mémoire du switch pour le routage en remplaçant le modèle de gestion de base de données SDM (Switch Database Management) à partir du modèle par défaut par le modèle Lanbase Routing.
2. Activez le routage connecté uniquement.

   ou

   Activez et configurez le routage statique qui active le routage connecté par défaut.

Gestion de la configuration

Le switch peut conserver sa configuration dans la mémoire interne ou sur une carte SD externe. Par défaut, la carte SD a toujours la priorité sur la mémoire interne. Si une image et des fichiers de configuration valides de votre IOS sont disponibles sur la carte SD et que vous démarrez le switch avec la carte SD insérée, le switch charge les fichiers de la carte SD.

En général, la méthode de démarrage du switch devient la source de toutes les modifications apportées à la configuration. Par exemple, en cas de démarrage à partir de la carte SD, les changements que vous faites sont enregistrés sur la carte SD. Si vous démarrez le switch à partir de la mémoire interne, même si vous insérez une carte SD au démarrage du système, les modifications sont enregistrées dans la mémoire interne. Pour déterminer la méthode de démarrage, cliquez sur l'onglet SD Sync depuis l'interface Internet de Device Manager.

Les fichiers de configuration (config.text et vlan.dat) sont au format ASCII lisible par l'homme. Vous pouvez télécharger les fichiers sur un ordinateur en utilisant l'une des méthodes suivantes :

- FTP
- AOP
- À l'aide d'un ordinateur pour lire la carte SD

Vous pouvez également stocker les fichiers de configuration dans le cadre de votre projet de commande dans l'application Logix Designer.

L'interface Internet de Device Manager vous permet de synchroniser automatiquement ou à la demande l'image et les fichiers de configuration de votre IOS.

Synchronisation de la carte SD

La fonctionnalité de synchronisation de la carte SD vous permet de synchroniser la carte SD avec la mémoire flash intégrée. Vous pouvez synchroniser les fichiers de configuration ou l'image de l'IOS. Si la carte SD est présente, le switch démarre à partir de la carte SD avec sa configuration. Si la carte SD n'est pas présente, le switch lit les paramètres de démarrage à partir de l'image IOS spécifiée, conservée dans la mémoire interne.

IMPORTANT Vous pouvez écraser votre configuration souhaitée si vous synchronisez dans la mauvaise direction.

Alarmes

Vous pouvez connecter jusqu'à deux entrées d'alarme à partir de dispositifs externes dans votre environnement, comme une porte ou une jauge de température, au port d'entrée d'alarme sur le panneau avant du switch. Les contacts d'alarme de sortie peuvent être configurés à l'aide de l'interface CLI. La sortie par défaut est également déclenchée par une alarme de température trop basse/élevée ou un port sans condition de transfert. Le relais d'alarme de sortie peut être configuré comme un circuit normalement sous tension ou normalement hors tension à l'aide de l'interface CLI.

Logiciel de l'IOS cryptographique (facultatif)

L'IOS cryptographique Stratix 5700 (disponible au téléchargement sous une référence distincte) assure la sécurité du réseau en chiffrant le trafic de l'administrateur au cours des sessions Telnet et SNMP. L'IOS cryptographique prend en charge toutes les fonctionnalités de l'IOS standard, ainsi que les protocoles suivants :

- Secure Shell (SSH) Protocol v2
- SNMPv3
- HTTPS

Diagnostic des câbles

La fonction de diagnostic des câbles vous permet d'exécuter un test sur chaque port du switch afin de déterminer l'intégrité du câble connecté aux ports RJ45 (cuivre). Cette fonctionnalité n'est pas disponible pour les ports en fibre.

Le test détermine la distance de rupture de câble du switch pour chaque câble et indique une valeur d'erreur individuelle.

Fonctionnalités avancées du logiciel

Des fonctionnalités logicielles avancées sont disponibles. Certaines sont configurées par la macro globale ou les smartports pour les applications d'automatisation type décrites dans ce manuel.

Pour plus d'informations sur la façon de configurer les fonctionnalités indisponibles dans l'interface Internet de Device Manager ou l'application Logix Designer, consultez :

- Le manuel Cisco IE2000 Switch Software Configuration sur le site http://www.Cisco.com.
- Le manuel Cisco IE2000 Switch Command-Line Interface Manual sur le site http://www.Cisco.com.

Gestion du switch via l'interface Internet de Device Manager

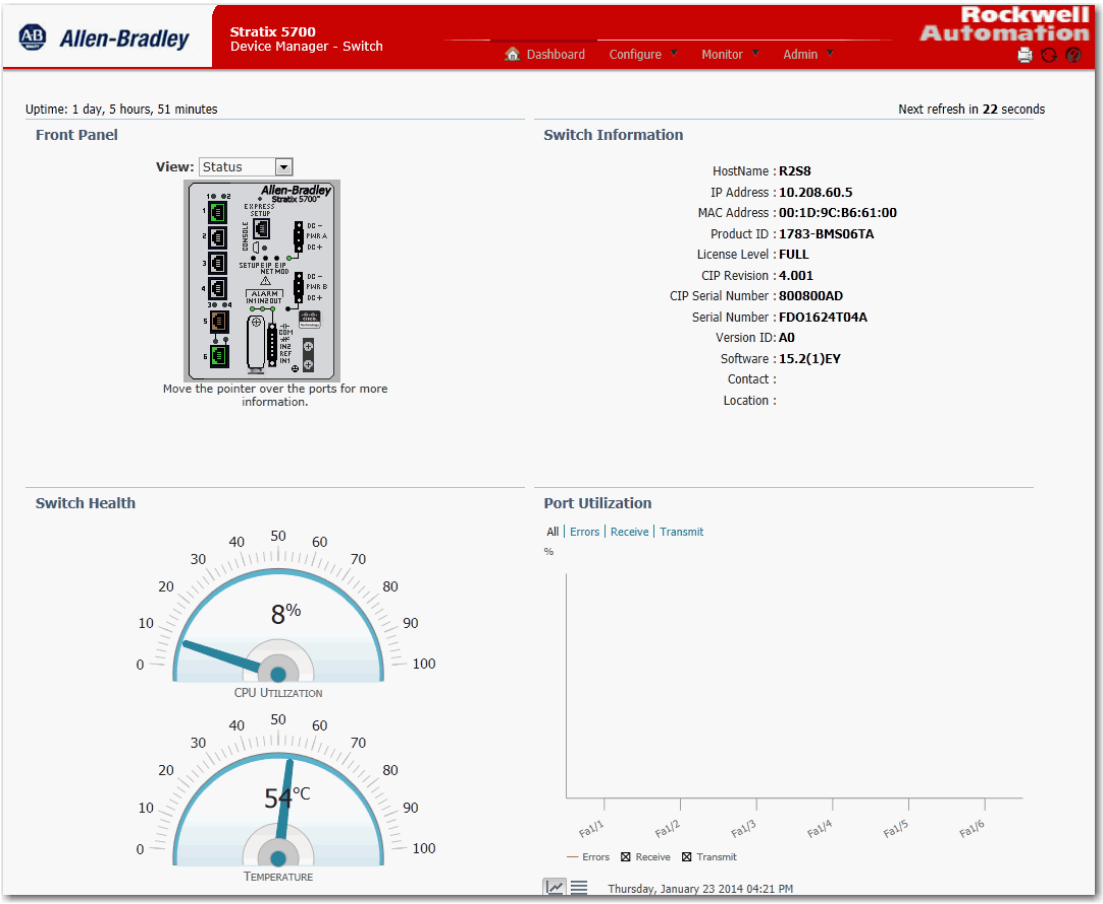
Après avoir terminé Express Setup, vous pouvez gérer le switch à l'aide de l'interface Internet de Device Manager fourni avec le switch.

Pour plus de simplicité, la plupart des illustrations dans ce chapitre montrent un switch à 6 ports.

Accès à l'interface Internet de Device Manager

Pour accéder à l'interface Internet de Device Manager, suivez les étapes ci-après.

1. Lancez un navigateur Internet sur votre poste de travail.
2. Entrez l'adresse IP du switch dans le navigateur Internet, puis cliquez sur Entrée.
3. Entrez le nom d'utilisateur et le mot de passe.



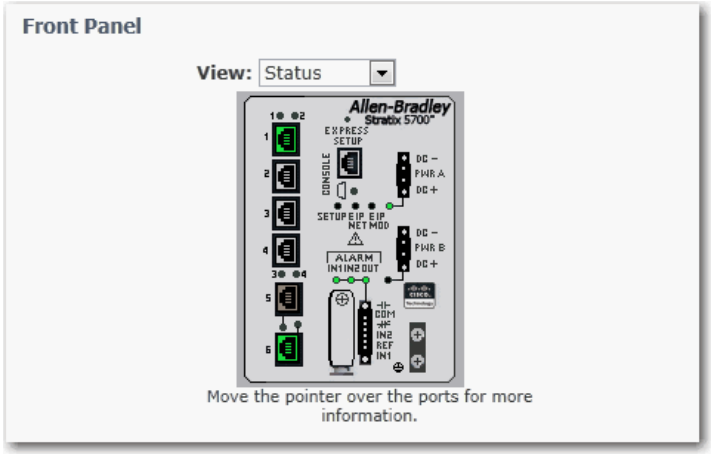
Présentation du tableau de bord

Vous pouvez utiliser le tableau de bord pour surveiller l'état et les performances du switch.

La fenêtre du tableau de bord est similaire à la fenêtre Monitor > Trends. La fenêtre du tableau de bord affiche l'état instantané, tandis que la fenêtre Trends affiche l'état historique. Les utiliser ensemble vous permet de rassembler les conditions détaillées du switch et de ses ports. Pour plus d'informations sur la fenêtre Trends, voir page 145.

Face avant et voyants d'état

La vue Front Panel (face avant) est un affichage graphique des faces avant du switch.



Les composants du switch sur la face avant sont chromocodés par état. Les couleurs vous aident à voir rapidement s'il existe un défaut ou une condition d'erreur. Les voyants -d'état au niveau du système et les voyants d'état au niveau du port, représentés sur la face avant correspondent à ceux du switch physique.

Tableau 8 - Voyants d'état de la face avant

Voyant	Etat	Description
EIP Mod	Le voyant d'état EIP Mod indique l'état du switch.	
	Éteint	L'alimentation du switch est éteinte, ou elle n'est pas correctement branchée.
	Vert fixe	Le switch fonctionne correctement.
	Vert clignotant	Le switch n'est pas configuré (par exemple, aucune adresse IP n'est configurée pour le switch).
	Rouge clignotant	Le switch a détecté une erreur système récupérable.
	Rouge fixe	Le switch a détecté une erreur système irrécupérable.
	Vert et rouge clignotant	Le switch est en train de réaliser son autotest de mise sous tension (POST).
DC_A DC_B	Éteint	L'alimentation du switch est éteinte, ou elle n'est pas correctement branchée.
	Vert fixe	L'alimentation est présente sur le circuit associé.
	Rouge fixe	L'alimentation n'est pas présente sur le circuit associé et le switch est configuré pour l'alimentation à double entrée.
Alarm Out	Éteint	Alarm Out non configuré, ou le switch est éteint.
	Vert fixe	Alarm Out est configuré ; aucune alarme n'est détectée.
	Rouge clignotant	Le switch a détecté une alarme majeure.
Alarm In 1 Alarm In 2	Éteint	Entrée d'alarme non configurée.
	Vert fixe	Entrée d'alarme configurée ; aucune alarme détectée.
	Rouge clignotant	Alarme majeure détectée.
	Rouge fixe	Alarme mineure détectée.

Tableau 8 - Voyants d'état de la face avant (suite)

Voyant	Etat	Description
Setup	Éteint	Le switch est configuré comme un switch administré.
	Vert fixe	Le switch est en configuration initiale.
	Vert clignotant	Le switch est en configuration initiale, en récupération après défaut ou la configuration initiale n'est pas terminée.
	Rouge fixe	Le switch n'a pas pu démarrer la configuration initiale ou la récupération, car il n'y a aucun port de switch disponible pour se connecter à la station de gestion. Débranchez un dispositif d'un port de switch, puis appuyez sur le bouton Express Setup du switch.
Ports : chaque port mixte a deux voyants d'état : un pour le module SFP et un pour le connecteur RJ45. Le voyant d'état approprié est actif pour le port actif.		
	Éteint	Aucune liaison présente sur le port.
	Vert fixe	Liaison ; aucune activité.
	Vert clignotant et éteint	La liaison est active et saine.
	Vert et orange en alternance	Il y a un défaut ou erreur sur la liaison.
	Jaune fixe	Le port est désactivé.
EIP Net : le voyant d'état EIP Net indique l'état du réseau du switch.		
	Éteint	L'alimentation du switch est éteinte, ou elle n'est pas correctement branchée.
	Vert fixe	Le switch a une connexion CIP établie avec un ou plusieurs dispositifs connectés.
	Vert clignotant	Le switch a une adresse IP, mais pas de connexion établie avec un ou plusieurs dispositifs connectés.
	Rouge clignotant	Une ou plusieurs connexions aux dispositifs connectés a(ont) expiré.
	Rouge fixe	Le switch a détecté que son adresse IP était déjà utilisée par un autre dispositif sur le réseau.
	Vert et rouge clignotant	Le switch est en train de réaliser son autotest de mise sous tension (POST).
Status : dans ce mode, les voyants d'état de port indiquent l'état des ports. Il s'agit du mode par défaut.		
	Éteint	Aucune liaison.
	Vert fixe	Aucune activité sur la liaison.
	Vert clignotant	Activité sur la liaison.
	Brun fixe	Le port a été désactivé.
	Jaune	Une erreur a désactivé le port.
	Vert et jaune clignotant	Liaison défectueuse.
	Jaune clignotant	Discordance de configuration de Smartports sur le port.
	Jaune fixe	Le port est défectueux, désactivé en raison d'une erreur, ou dans un état de blocage par le protocole STP.
Smartports : dans ce mode, chaque image de port indique le rôle de port appliqué. Pour plus d'informations à propos de Smartports, voir Optimiser les ports grâce aux rôles des ports smartport à la page 64.		

Vous pouvez modifier le comportement du voyant d'état de port en choisissant un mode Port dans la liste View de la face avant.

Déplacez le pointeur sur un port pour afficher des informations spécifiques sur le port et son état.

CONSEIL Si vous déplacez le pointeur sur un port qui clignote en vert et jaune, l'état est l'une des conditions suivantes :

- La liaison est défectueuse
- La liaison présente des collisions

Dans l'un comme dans l'autre, le port reçoit et envoie du trafic.

Notez les points suivants :

- La vitesse et le mode Duplex pour un port apparaissent uniquement lorsqu'un dispositif est connecté au port.
- Pour les ports à double fonction, le champ Type affiche 10/100/1 000BaseTX pour le port de liaison montante en cuivre que le port soit actif ou pas. Le champ Type affiche également soit le type de module SFP installé, soit Empty si aucun module n'est installé.
- Le type de Smartport, ainsi que le type et le nom de VLAN sont affichés lorsque le mode Smartport Port est sélectionné.
- Le champ Uptime indique combien de temps le switch a fonctionné depuis sa dernière mise sous tension ou son dernier redémarrage. Status est rafraîchi automatiquement toutes les 60 secondes ou lorsque vous cliquez sur Refresh. Le compteur d'actualisation indique le nombre de secondes qui restent avant le début du prochain cycle de rafraîchissement.

Informations sur le switch

La zone Switch Information du tableau de bord affiche des informations sur le switch, comme décrit dans le tableau ci-dessous.

Champ	Description
Host Name	Un nom descriptif pour ce switch. Le nom par défaut est Switch. Vous pouvez définir ce paramètre dans la fenêtre Admin > Express Setup.
IP Address	L'adresse IP de ce switch. Vous pouvez configurer ce paramètre dans la fenêtre Admin > Express Setup.
MAC Address	L'adresse MAC de ce switch. Cette information ne peut pas être modifiée.
Product ID	Le modèle de ce switch. Cette information ne peut pas être modifiée.
License Level	Le type de licence qui est installé. Cette information ne peut pas être modifiée.
CIP Revision	La version de protocole industriel commun (CIP) qui est prise en charge sur ce switch. Cette information ne peut pas être modifiée.
CIP Serial Number	Le numéro de série CIP. Cette information ne peut pas être modifiée.
Serial Number	Le numéro de série de ce switch. Cette information ne peut pas être modifiée.
Version ID	La version du matériel. Cette information ne peut pas être modifiée.
Software	La version d'IOS que ce switch exécute. Cette information est mise à jour lorsque vous mettez à niveau le firmware du switch.
Contact	La personne qui est le contact administratif pour ce switch. Vous pouvez définir ce paramètre dans la fenêtre Configure > SNMP.
Location	L'emplacement physique de ce switch. Vous pouvez définir ce paramètre dans la fenêtre Configure > SNMP.

Santé du switch

Vous pouvez utiliser les jauges de santé pour surveiller le switch.

Utilisation de l'unité centrale

La jauge CPU Utilization indique le pourcentage de la puissance de traitement de l'unité centrale utilisée sur le switch. Des données sont collectées à chaque rafraîchissement de système toutes les 60 secondes. La jauge est modifiée à mesure que le switch expérimente l'activité réseau à partir des dispositifs qui envoient des données à travers le réseau. À mesure que l'activité réseau augmente, il y a de plus en plus de conflit entre les dispositifs pour envoyer des données à travers le réseau.

Lorsque vous surveillez l'utilisation sur le switch, notez si le pourcentage d'utilisation correspond à ce à quoi vous vous attendiez pendant ce temps donné de l'activité réseau. Si l'utilisation est élevée alors que vous vous attendiez à ce qu'elle soit basse, il y a peut-être un problème. Lorsque vous surveillez le switch, notez si l'utilisation de bande passante est constamment élevée. Cela peut signifier qu'il y a de la congestion dans le réseau. Si le switch atteint sa bande passante maximale (utilisation supérieure à 90 %) et que ses mémoires tampons sont pleines, il commence à jeter les paquets de données qu'il reçoit. Une perte de paquets dans le réseau n'est pas considérée comme inhabituelle et le switch est configuré pour aider à récupérer les paquets perdus, en demandant par exemple aux autres dispositifs de renvoyer les données. Toutefois, une perte de paquets excessive peut créer des erreurs de paquets qui peuvent à leur tour dégrader les performances globales du réseau.

Pour réduire la congestion, vous pouvez envisager de segmenter le réseau en sous-réseaux connectés par d'autres switchs ou routeurs. Recherchez d'autres causes, telles que les connexions ou dispositifs défectueux qui peuvent également augmenter l'utilisation de bande passante sur le switch.

Température

La jauge Temperature indique la température interne du switch. Pour plus d'informations sur la plage de températures du switch et les directives relatives à l'environnement de fonctionnement, reportez-vous à la publication 1783-TD001, Stratix Ethernet Device Specifications Technical Data.

Utilisation du port

Vous pouvez choisir quels types de trafic de réseau afficher et sous quel format :

- Types de trafic : par défaut, l'ensemble du trafic est affiché pour toutes les interfaces. Cliquez sur les liens au-dessus de la zone d'affichage pour afficher tout le trafic, les erreurs, le trafic reçu ou le trafic transmis.
- Formats : cliquez sur les boutons en dessous de la zone d'affichage pour afficher les données en Chart Mode ou Grid Mode.
- Détails de graphique : lors de l'affichage d'un graphique, placez le pointeur de votre souris sur une barre ou un point sur le graphique pour afficher les données correspondantes.

Lorsque vous surveillez l'utilisation des ports, notez si le pourcentage correspond à ce à quoi vous vous attendiez pendant ce moment donné de l'activité réseau. Si l'utilisation est élevée alors que vous vous attendiez à ce qu'elle soit basse, il y a peut-être un problème. L'allocation de bande passante peut également être basée sur le mode de fonctionnement de la connexion (Half-duplex ou Full-duplex).

Vous trouverez ci-dessous quelques-unes des erreurs reçues par les ports du switch ou envoyées par ceux-ci :

- Mauvaise connexion de câble
- Ports défectueux
- Problèmes de logiciel
- Problèmes de driver

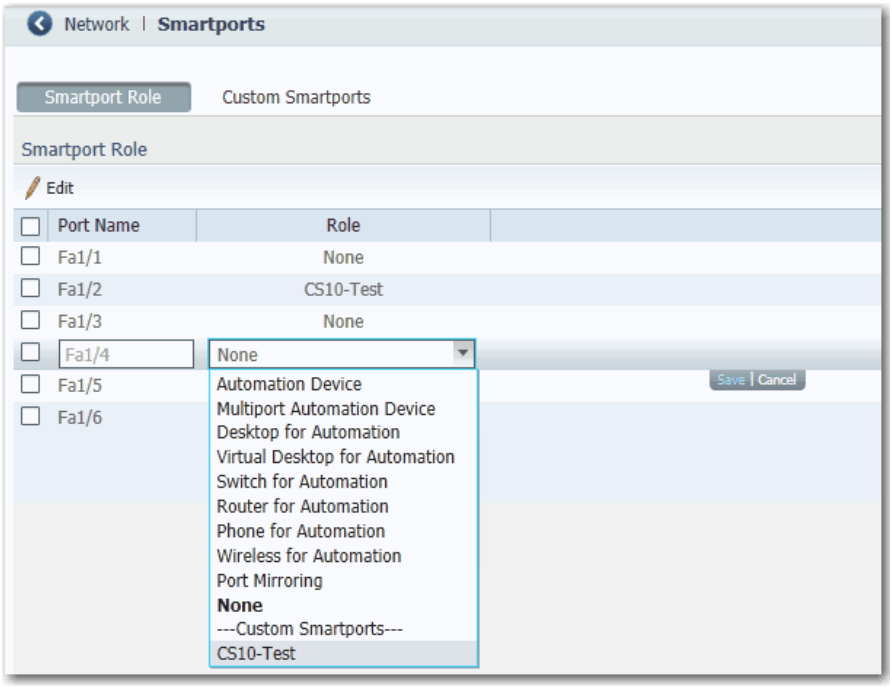
Des données sont collectées à chaque rafraîchissement de système toutes les 60 secondes.

Reportez-vous à la section Surveillance des tendances à la page 145 pour un graphique permettant d'afficher des modèles port par port au cours des instances incrémentielles exprimées en temps (par 60 secondes, 1 heure, 1 jour ou 1 semaine).

Reportez-vous à la section Surveillance des statistiques de port à la page 146 pour plus de détails sur les erreurs de port spécifiques détectées sur chaque port.

Configuration des Smartports

Pour affecter des rôles Smartport aux ports du switch, dans le menu Configure, choisissez Smartports.



Suivez ces directives lorsque vous utilisez des rôles Smartport :

- Avant d'utiliser des rôles Smartport, décidez quel port du switch est connecté à quel type de dispositif.
- Avant de brancher un dispositif au port ou de rebrancher les dispositifs qui ont été déplacés, vérifiez quel rôle Smartport est appliqué à un port.

IMPORTANT	Nous recommandons de ne pas modifier les paramètres de port après avoir activé un rôle Smartport sur un port. Toute modification de paramètres de port peut altérer l'efficacité du rôle Smartport.

- Lorsque l'utilisateur tente d'appliquer un rôle de port à un port acheminé dans la fenêtre Smartports, ce message d'erreur s'affiche :

  « A port role cannot be configured on a routed port » (un rôle de port ne peut pas être configuré sur un port acheminé).

Pour appliquer un rôle Smartport, suivez la procédure ci-après.

1. Dans le menu Configure, choisissez Smartports.
2. Sélectionnez un port.
3. Choisissez un rôle Smartport dans le menu déroulant de la colonne Role.
4. Cliquez sur Save (enregistrer).

Personnaliser les attributs du rôle de port

Chaque port de switch est membre d'un VLAN. Les dispositifs connectés aux ports de switch qui appartiennent au même VLAN partagent les mêmes diffusions générales de données et ressources système.

Selon vos exigences de réseau, il peut être suffisant d'affecter tous les ports au VLAN par défaut qui est nommé default. Un seul VLAN peut être suffisant pour un petit réseau.

Avant de changer les appartenances au réseau local virtuel (VLAN), comprenez ce qu'est un VLAN, son but et comment créer un VLAN. Voir page 70 pour plus d'informations sur les VLAN.

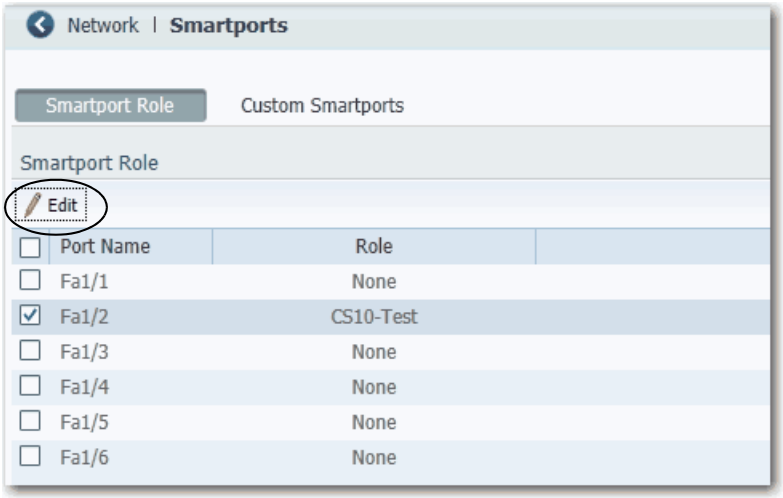
Affecter un port à un VLAN (appartenances au VLAN)

Chaque port de switch est membre d'un VLAN. Les dispositifs connectés aux ports de switch qui appartiennent au même VLAN partagent les mêmes diffusions générales de données et ressources système. La communication entre les VLAN nécessite un dispositif de couche 3 (tel qu'un routeur ou un switch de couche 3).

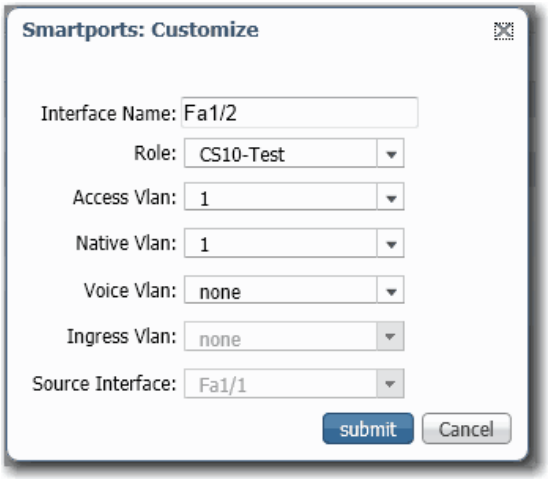
Selon vos exigences de réseau, il peut être suffisant d'affecter tous les ports au VLAN par défaut qui est nommé Default. Si des VLAN supplémentaires ont été créés, vous devez décider quels ports sont les mieux adaptés à quels VLAN.

Pour modifier une affectation à un VLAN, suivez les étapes ci-après.

1. Dans le menu Configure, choisissez Smartports.
2. Cochez la case en regard du port dont vous allez modifier le VLAN.
3. Cliquez sur Edit.



4. Modifiez les affectations de VLAN comme nécessaire :
   - Pour les ports appliqués avec le rôle de port Automation Device with QoS, Switch For Automation, Router For Automation ou Wireless For Automation, choisissez un VLAN dans la liste Native VLAN.
   - Pour les ports appliqués avec le rôle de port Automation Device, Desktop For Automation, Phone For Automation ou None, choisissez un VLAN dans la liste Access VLAN.
   - Pour les ports appliqués avec le rôle de port Phone For Automation, choisissez un VLAN dans la liste Voice VLAN.
   - Pour les ports appliqués avec le rôle de port Port Mirroring, choisissez un VLAN de la liste Ingress VLAN, puis choisissez le port à surveiller dans la liste Source Interface.



5. Cliquez sur Submit (soumettre).

Gérer des macros Smartport personnalisées

Pour créer une macro Smartport personnalisée, suivez les étapes ci-après.

1. Cliquez sur l'onglet Custom Smartports.
2. Cliquez sur Add.
3. Entrez le nom pour la macro.

   Les noms de macro sont sensibles à la casse. La chaîne peut comporter jusqu'à 31 caractères alphanumériques. La chaîne ne peut pas contenir un ?, un espace ou une tabulation.
4. Choisissez une icône de macro (CS1 à CS10).

5. Entrez une définition de macro.

   La définition peut contenir jusqu'à 3000 caractères. Entrez les commandes de macro avec une commande par ligne. Utilisez le caractère # au début d'une ligne pour saisir le texte du commentaire à l'intérieur de la macro.

   Les paramètres disponibles pour la macro sont $native_vlan, $access_vlan et $voice_vlan.

6. Entrez une définition d'antimacro.

   La définition d'antimacro est la partie de la macro appliquée qui supprime la macro lorsque vous la changez en une autre macro, ou lorsque vous l'enlevez avec le rôle Smartport « None ». Avant que la définition de macro ne puisse être appliquée au port, l'antimacro doit d'abord être définie avec les commandes appropriées pour remettre le port à son état initial.

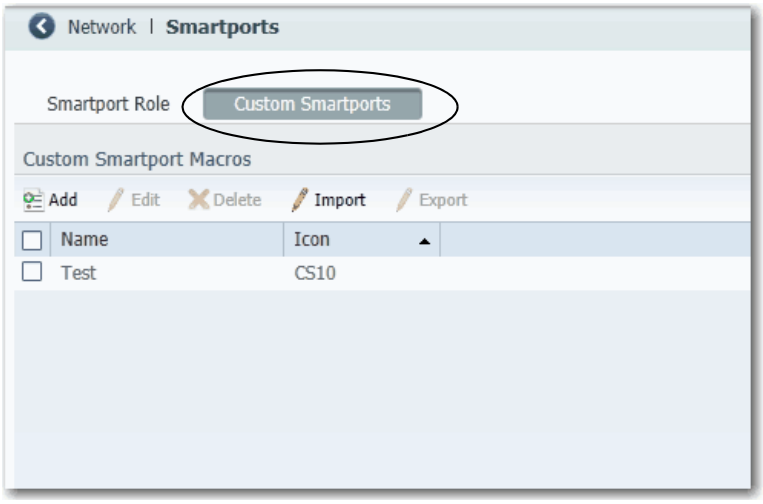
   La définition peut contenir jusqu'à 3000 caractères. Entrez les commandes d'antimacro avec une commande par ligne. Utilisez le caractère @ à la fin de la macro. Utilisez le caractère # au début d'une ligne pour saisir le texte du commentaire à l'intérieur de la macro.

7. Cliquez sur Submit (soumettre).
8. Pour ignorer toutes les modifications non sauvegardées, cliquez sur Cancel (annuler).

Modifier la définition d'une macro Smartport personnalisée

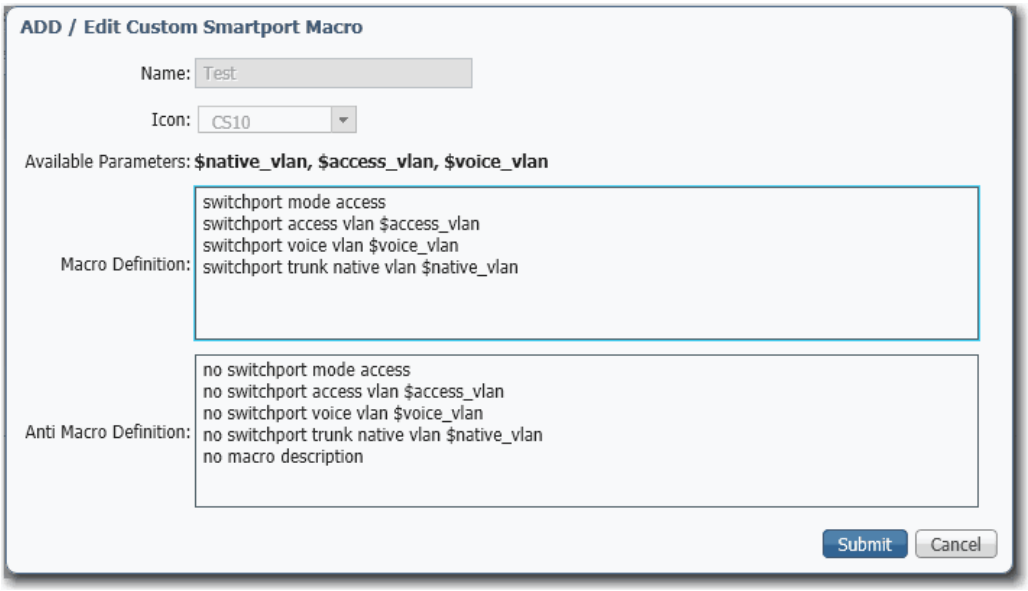
Vous ne pouvez pas modifier une macro Smartport personnalisée qui est en cours d'utilisation.

1. Dans le menu Configure, choisissez Smartports.
2. Cliquez sur l'onglet Custom Smartports.



3. Cochez la case à côté de la macro à modifier.

4. Cliquez sur Edit.

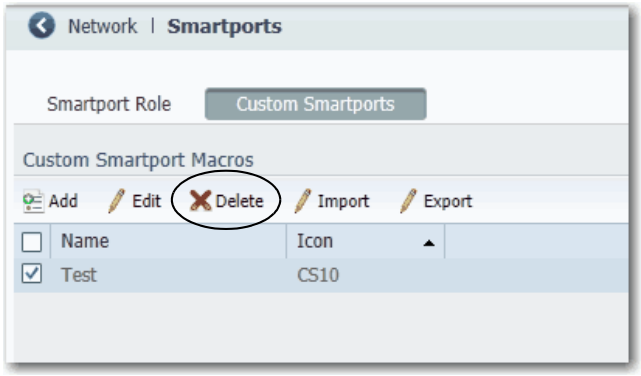


5. Modifiez les définitions comme nécessaires.
6. Cliquez sur Submit (soumettre).

Supprimer une macro Smartport personnalisée

Vous ne pouvez pas supprimer une macro Smartport personnalisée qui est en cours d'utilisation.

1. Dans le menu Configure, choisissez Smartports.
2. Cliquez sur l'onglet Custom Smartports.
3. Cochez la case située en regard de la macro à supprimer.

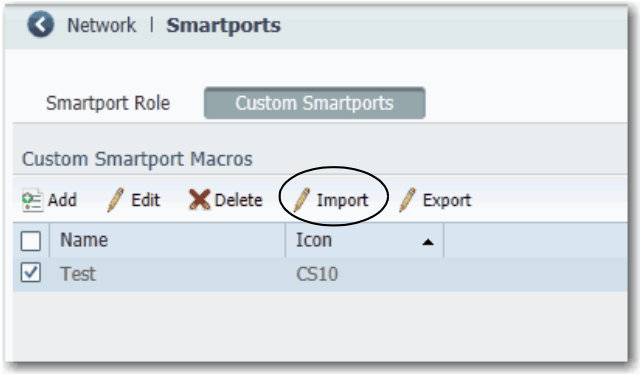


4. Cliquez sur Delete (effacer).

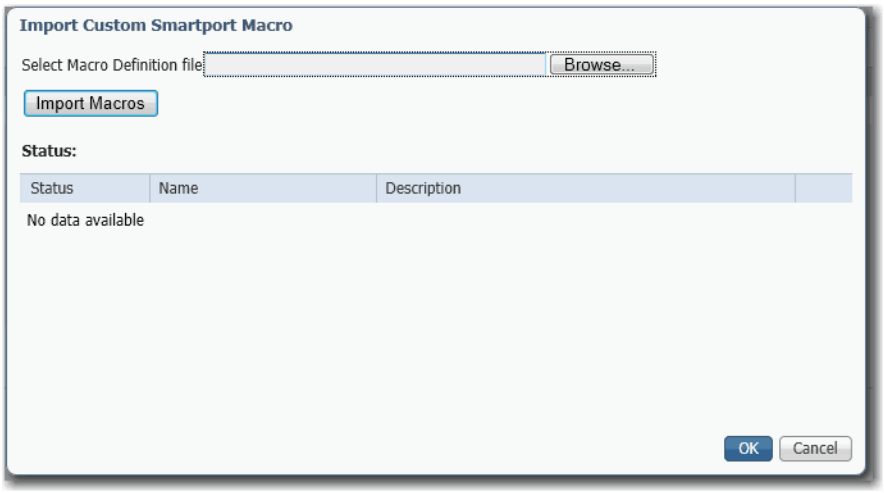
Importer une macro Smartport personnalisée

Vous devez utiliser Firefox 3.6 ou supérieur pour importer une macro Smartport personnalisée.

1. Dans le menu Configure, choisissez Smartports.
2. Cliquez sur l'onglet Custom Smartports.
3. Cliquez sur Import.



4. Cliquez sur Browse (parcourir).



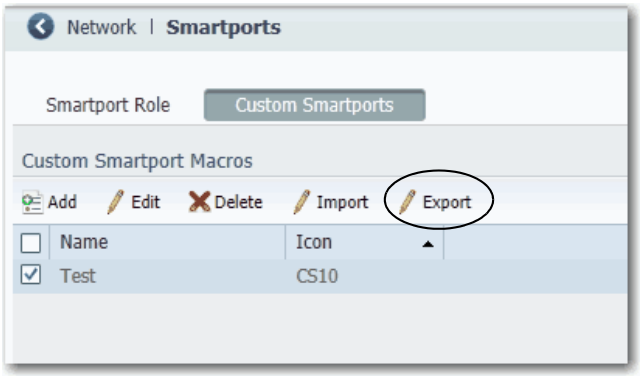
5. Sélectionnez le fichier de macro sur votre ordinateur ou lecteur réseau.

   Le fichier doit être un fichier au format .xml.
6. Cliquez sur Import Macros.
7. Cliquez sur OK.

Exporter une macro Smartport personnalisée

Vous devez utiliser Firefox 3.6 ou supérieur pour exporter une macro Smartport personnalisée.

1. Dans le menu Configure, choisissez Smartports.
2. Cliquez sur l'onglet Custom Smartports.
3. Cochez la case située en regard de la macro à exporter.
4. Cliquez sur Export.

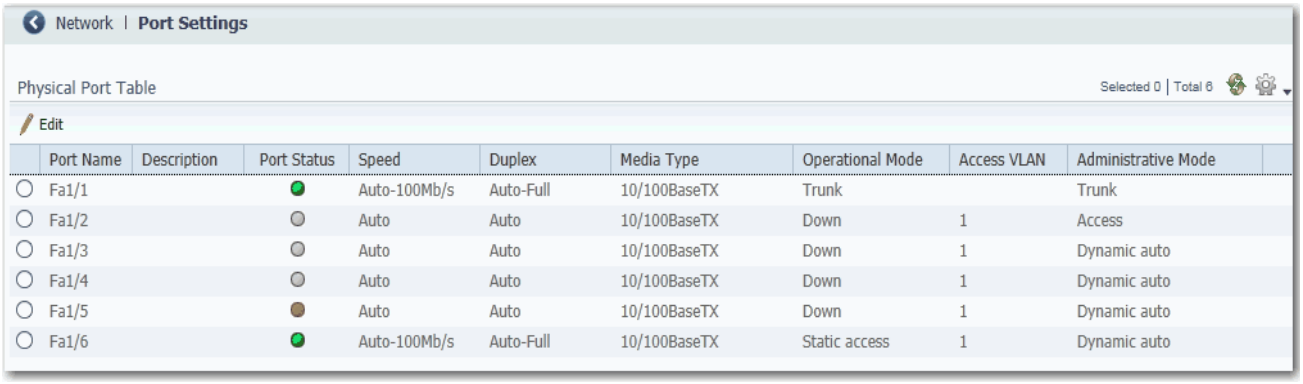


5. Enregistrez le fichier obtenu.

Configuration des paramètres de port

Les paramètres de port de base déterminent comment les données sont reçues et envoyées entre le switch et le dispositif connecté. Vous pouvez modifier ces paramètres pour les adapter à vos besoins en matière de réseau et pour résoudre des problèmes de réseau. Les réglages d'un port de switch doivent être compatibles avec les réglages de port du dispositif connecté.

Pour modifier les réglages de port de base, dans le menu Configure, choisissez Port Settings (réglages de port).



	Port Name	Description	Port Status	Speed	Duplex	Media Type	Operational Mode	Access VLAN	Administrative Mode
○	Fa1/1		●	Auto-100Mb/s	Auto-Full	10/100BaseTX	Trunk		Trunk
○	Fa1/2		●	Auto	Auto	10/100BaseTX	Down	1	Access
○	Fa1/3		●	Auto	Auto	10/100BaseTX	Down	1	Dynamic auto
○	Fa1/4		●	Auto	Auto	10/100BaseTX	Down	1	Dynamic auto
○	Fa1/5		●	Auto	Auto	10/100BaseTX	Down	1	Dynamic auto
○	Fa1/6		●	Auto-100Mb/s	Auto-Full	10/100BaseTX	Static access	1	Dynamic auto

Tableau 9 liste les réglages de base pour les ports du switch. Pour modifier ces réglages, cliquez sur le bouton radio en regard du nom de port, puis cliquez sur Edit pour afficher la fenêtre Edit Physical Port.

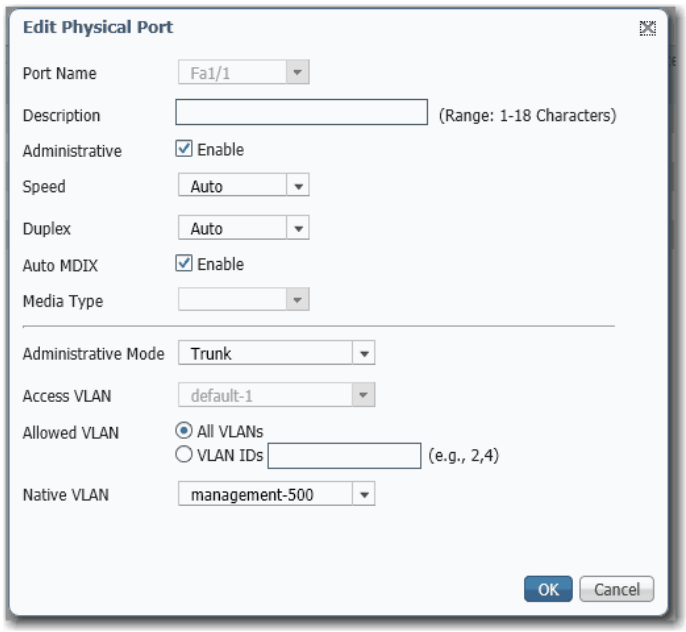


Tableau 9 - Réglages de port

Champ	Description
Port Name	Le numéro du port de switch, comprenant le type de port (Fa pour Fast Ethernet et Gi pour Gigabit Ethernet) et le numéro de port spécifique : • GI/1 est le port Gigabit 1 du switch. • FA1/1 est le port Fast Ethernet 1 sur le switch.
Description	La description du port de switch. Nous vous recommandons de fournir une description de port pour permettre d'identifier le port au cours de la surveillance et du dépannage. La description peut être l'emplacement du dispositif connecté ou le nom de la personne utilisant le dispositif connecté.
Port Status	L'état du port de switch. La valeur par défaut est Enabled (activé). Vous pouvez modifier ce réglage dans la fenêtre Edit Physical Port en cochant ou décochant la case Administrative. Nous recommandons de désactiver le port s'il n'est pas utilisé et n'est pas relié à un dispositif. Ce réglage pourra par exemple être modifié pendant un dépannage. Vous pouvez dépanner une connexion non autorisée en désactivant administrativement le port.
Speed	La vitesse de fonctionnement du port de switch. Vous pouvez choisir Auto (autonégociation) si le dispositif connecté peut négocier la vitesse de la liaison avec le port de switch. La valeur par défaut est Auto. Nous recommandons d'utiliser la valeur par défaut, de sorte que le réglage de vitesse sur le port de switch corresponde automatiquement au paramètre sur le dispositif connecté. Modifiez la vitesse du port de switch si le dispositif connecté requiert une vitesse spécifique. Ce réglage pourra par exemple être modifié pendant un dépannage. Si vous dépannez un problème de connectivité, vous pouvez modifier ce réglage pour voir si le port de switch et le dispositif connecté ne présentent pas la même vitesse.
Duplex	Le mode Duplex du port de switch : • Auto (autonégociation) si le dispositif connecté peut négocier avec le switch. • Full (mode Full-duplex) si les deux dispositifs peuvent envoyer des données en même temps. • Half (mode Half-duplex) si un des dispositifs ou les deux ne peuvent pas envoyer des données en même temps. La valeur par défaut est Auto. Sur les ports Gigabit Ethernet, vous ne pouvez pas définir le port sur le mode Half-duplex si la vitesse du port est définie sur Auto. Nous vous recommandons d'utiliser la valeur par défaut afin que le réglage sur le port de switch corresponde automatiquement au paramètre sur le dispositif connecté. Changez le mode Duplex sur le port de switch si le dispositif connecté requiert un mode spécifique. Ce réglage pourra par exemple être modifié pendant un dépannage. Si vous dépannez un problème de connectivité, vous pouvez modifier ce réglage pour voir si le port de switch et le dispositif connecté n'utilisent pas le même mode duplex.
Auto-MDIX	Permet de définir si la fonction de croisement automatique d'interface dépendant du support (auto-MDIX) peut détecter automatiquement le type de connexion de câble requis (droit ou croisé) et configurer la connexion de manière appropriée. La valeur par défaut est Enable (validé). Ce réglage n'est pas disponible sur les ports de module SFP.
Media Type	Le type de port actif (le port RJ45 ou le port de module SFP) d'un port de liaison montante à double fonction. Par défaut, le switch détecte si le port RJ45 ou le port de module SFP d'un port à double fonction est connecté et utilise le port en conséquence. Il ne peut y avoir qu'un seul port actif à la fois. Si les deux ports sont connectés, le port de module SFP a la priorité. Vous ne pouvez pas modifier le réglage de priorité. Choisissez parmi les types de support suivants : • SFP : le port de module SFP est actif. Si vous choisissez cette option, la vitesse et le duplex affichent les réglages actuels et auto-MDIX affiche N/A. • RJ45 : le port RJ45 est actif. Si vous choisissez cette option, vous pouvez définir les valeurs de la vitesse, du duplex et d'auto-mdix. • Auto (autonégociation) : l'un ou l'autre port peut être actif. Si vous choisissez cette option, la vitesse et le duplex sont définis sur auto et auto-MDIX affiche N/A. La valeur par défaut est Auto.

Tableau 9 - Réglages de port (suite)

Champ	Description
Operational Mode	L'état de fonctionnement du port. Affiche le mode administratif ou Down (si désactivé).
Access VLAN	Le VLAN auquel une interface appartient et apporte du trafic lorsque la liaison est configurée ou agit comme une interface de non-agrégation.
Administrative Mode	Affiche l'un des modes administratifs suivants : • Access : l'interface est en mode de non-agrégation permanente et négocie pour convertir la liaison voisine en une liaison de non-agrégation, même si la liaison voisine est une interface d'agrégation. Si vous choisissez cette option, choisissez également un Access VLAN. Un port d'accès appartient à et transporte du trafic à un seul VLAN (sauf s'il est configuré comme un port Voice VLAN). • Trunk : l'interface est en mode d'agrégation permanente et négocie pour convertir la liaison voisine en une liaison d'agrégation, même si l'interface voisine n'est pas une interface d'agrégation. Si vous choisissez cette option, choisissez également s'il convient ou non d'autoriser tous les VLAN ou des VLAN ID spécifiés • Dynamic Auto : l'interface convertit la liaison en une liaison d'agrégation si l'interface voisine est réglée en mode Trunk ou Desirable. Ce mode est le paramètre par défaut. Si vous choisissez cette option, spécifiez un Access VLAN à utiliser lorsque la liaison est en mode Access. Spécifiez également s'il convient d'autoriser tous les VLAN ou des VLAN ID spécifiés lorsque la liaison est en mode Trunk. • Dynamic Desirable : l'interface convertit la liaison en une liaison d'agrégation si l'interface voisine est réglée en mode Trunk, Dynamic Desirable ou Auto. Si vous choisissez cette option, spécifiez un Access VLAN à utiliser lorsque la liaison est en mode Access. Choisissez également s'il convient d'autoriser tous les VLAN ou des VLAN ID spécifiés lorsque la liaison est en mode Trunk.

Configuration des seuils de port

Configurez les seuils de port pour éviter que le trafic sur un réseau local ne soit perturbé par une tempête de diffusion générale, de multidiffusion ou d'envoi individuel sur l'une des interfaces.

Pour configurer les seuils de port, dans le menu Configure, choisissez Port Thresholds.

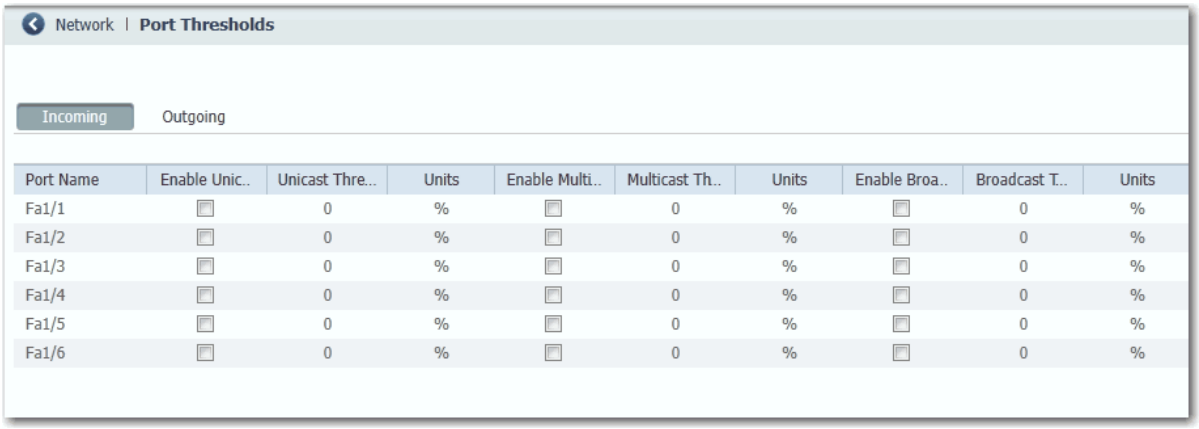


Tableau 10 - Champs de seuil de port

Champ	Description
Incoming (entrant)	
Unicast (envoi individuel) Multicast (multidiffusion) Broadcast (diffusion générale)	Pour chaque port, effectuez les opérations suivantes : 1. Cochez ou décochez la case Enable (valider). 2. Saisissez la valeur de seuil. 3. Choisissez l'une des unités ci-après : – PPS (0 à 10 milliards) – BPS (0 à 10 milliards) – % (0 à 100)
Outgoing (sortant)	
All Traffic	Pour chaque port, effectuez les opérations suivantes : 1. Cochez ou décochez la case Enable. 2. Saisissez la valeur de seuil. 3. Cliquez sur Save (enregistrer)

Configuration des EtherChannels

Un EtherChannel (ou groupe de ports) est un groupe d'au moins deux ports de switch regroupés en une seule liaison logique, créant ainsi une liaison de bande passante plus importante entre deux switchs.

Par exemple, quatre ports de switch 10/100 peuvent être affectés à un EtherChannel pour fournir la bande passante full-duplex pouvant atteindre 800 Mbits/s. Si l'un des ports du EtherChannel devient indisponible, le trafic est acheminé par les ports restants au sein de l'EtherChannel.

Tous les ports d'un EtherChannel doivent avoir les mêmes caractéristiques :

- Tous sont appliqués avec le rôle de port Smartports IE Switch et appartiennent au même VLAN.
- Tous sont soit des ports 10/100, soit des ports 10/100/1 000. Vous ne pouvez pas regrouper un mélange de ports 10/100 et 10/100/1 000 dans un EtherChannel.
- Tous sont activés. Un port désactivé dans un EtherChannel est traité comme un défaut de liaison et son trafic est transféré vers l'un des ports restants dans l'EtherChannel.

IMPORTANT N'activez pas les adresses de couche 3 sur les interfaces EtherChannel physiques.

Pour créer, modifier et supprimer des EtherChannels, dans le menu Configure, choisissez EtherChannels.

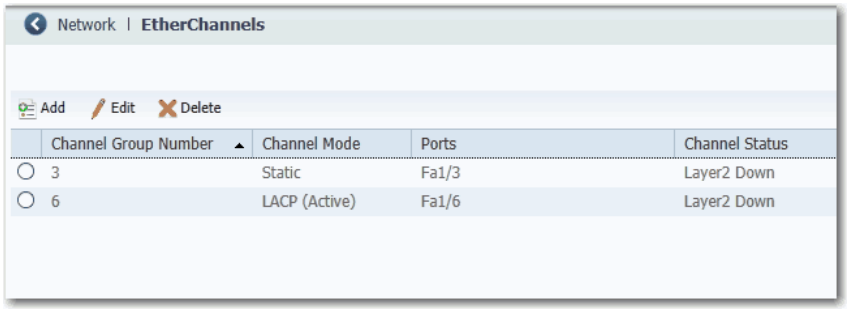


Tableau 11 - Champs d'EtherChannel

Champ	Description
Channel Group Number	Un numéro de 1 à 6 qui identifie cet EtherChannel. Vous pouvez configurer jusqu'à six EtherChannels.
Channel Mode	Détermine comment les ports deviennent actifs. Avec toutes les options sauf On, des négociations ont lieu pour déterminer les ports qui deviennent actifs. Les ports incompatibles sont mis dans un état indépendant et continuent à transporter du trafic de données, mais ne participent pas à l'EtherChannel. **IMPORTANT :** assurez-vous que tous les ports d'un EtherChannel sont configurés avec la même vitesse et le même mode duplex. Les modes disponibles sont : • Static : Tous les ports rejoignent l'EtherChannel, sans négociations. Ce mode peut être utile si le dispositif distant ne prend pas en charge les protocoles requis par les autres modes (voir ci-dessous). Les switchs aux deux extrémités de la liaison doivent être configurés en mode On. • PAgP : Ce mode active Port Aggregation Protocol (PAgP), un protocole propriétaire Cisco. Le port répond à des demandes de création d'EtherChannels, mais n'entame pas lesdites négociations. Ce mode « silencieux » est recommandé lorsqu'un port est relié à un dispositif, comme un serveur de fichiers ou un analyseur de paquets, qui n'enverra probablement pas des paquets PAgP. Un port en mode Auto peut former un EtherChannel avec un autre port en mode Desirable. • PAgP (non-silent) : ce mode est identique au mode Auto, mais est recommandé lorsque le port est relié à un dispositif qui devrait être actif dans le lancement d'EtherChannels. Un port en mode Auto peut former un EtherChannel avec un autre port en mode Desirable. • PAgP Desirable : ce mode active Port Aggregation Protocol (PAgP), un protocole propriétaire Cisco. Le port lance des négociations pour former des EtherChannels en envoyant des paquets PAgP à d'autres ports. Ce mode « silencieux » est recommandé lorsqu'un port est relié à un dispositif, comme un serveur de fichiers ou un analyseur de paquets, qui n'enverra probablement pas des paquets PAgP. Un port en mode Desirable peut former un EtherChannel avec un autre port en mode Desirable ou Auto. • PAgP Desirable (non-silent) : ce mode est identique au mode Desirable, mais est recommandé lorsque le port est relié à un dispositif qui devrait être actif dans le lancement d'EtherChannels. • LACP (Active) : ce mode active le protocole de contrôle d'agrégation de liaisons (LACP) sans condition. Le port envoie des paquets de LACP vers d'autres ports pour entamer des négociations dans le but de créer des EtherChannels. Un port en mode Active peut former un EtherChannel avec un autre port en mode Active ou Passive. Les ports doivent être configurés pour un duplex intégral. • LACP (Passive) : ce mode active le protocole de contrôle d'agrégation de liaisons (LACP) uniquement si un dispositif LACP est détecté à l'autre extrémité de la liaison. Le port répond à des demandes de création d'EtherChannels, mais n'entame pas lesdites négociations. Les ports doivent être configurés pour un duplex intégral.
Ports	Les ports qui peuvent participer à cet EtherChannel.
Channel Status	L'état du groupe.

Configuration de DHCP

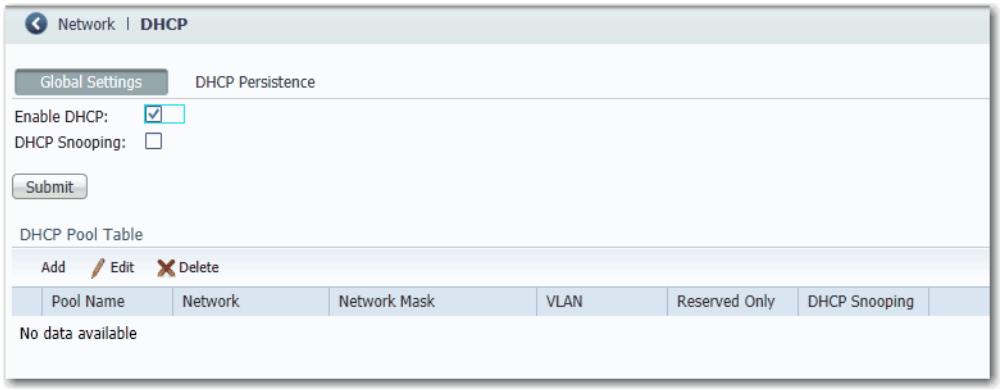
Pour utiliser la persistance DHCP, vous devez d'abord activer le DHCP et configurer le pool d'adresses IP. Ensuite, vous devez affecter des adresses IP spécifiques à chaque port.

Configurationdu serveur DHCP

Pour activer le mode DHCP Server sur le switch, effectuez les opérations suivantes :

1. Dans le menu Configure, choisissez DHCP.
2. Cochez la case Enable DHCP.
3. Pour activer la surveillance de trafic de DHCP, cochez la case DHCP Snooping.

   La surveillance de trafic de DHCP limite la diffusion de demandes de DHCP au-delà du switch connecté. Cela signifie que les dispositifs reçoivent des affectations de la part du switch connecté uniquement. Cette option est disponible uniquement sur les interfaces VLAN. Pour activer DHCP Snooping sur un VLAN spécifique, cochez la case DHCP Snooping pour le VLAN spécifique dans la table de pool DHCP.



4. Pour réserver un pool d'adresses uniquement aux dispositifs qui sont spécifiés dans le tableau de persistance de DHCP, cochez la case Reserved Only dans la table de pool DHCP.

   Les demandes de DHCP de la part des ports ne se trouvant pas dans la table de persistance ou de la part d'un autre dispositif (switch) sont ignorées. Par défaut, cette option est désactivée et la case Reserved Only est décochée.

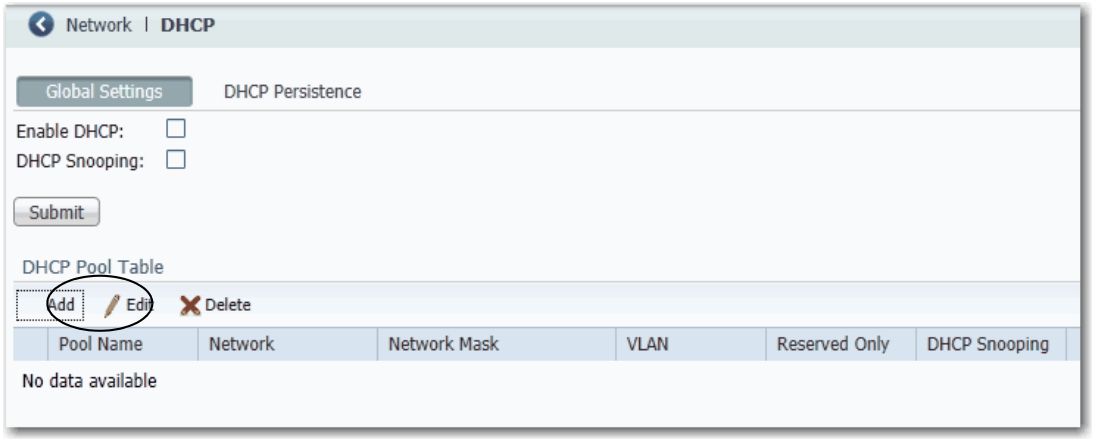
5. Cliquez sur Submit (soumettre).

Configurer un pool d'adresses IP DHCP

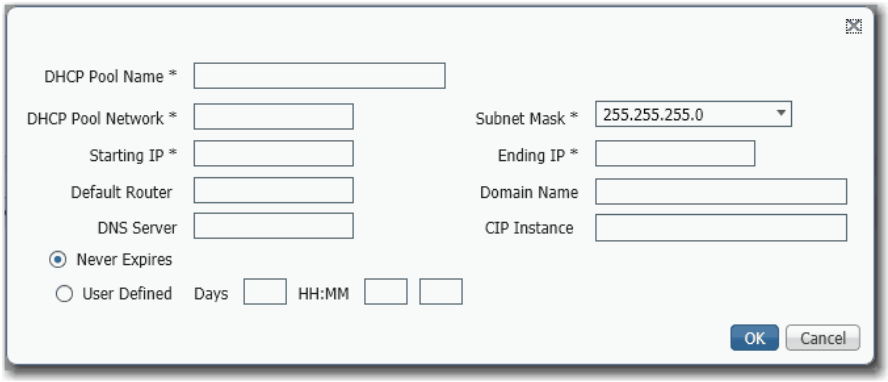
Une fois DHCP activée, vous pouvez créer le pool d'adresses correspondant.

Pour configurer un pool d'adresses IP DHCP, procédez comme suit :

1. Dans le menu Configure, choisissez DHCP.
2. Cliquez sur Add.



3. Renseignez les champs comme indiqué ci-dessous, puis cliquez sur OK.



Champ	Description
DHCP Pool Name	Le nom du pool d'adresses IP DHCP configuré sur le switch. Le nom peut compter jusqu'à 31 caractères alphanumériques. Le nom ne peut pas contenir un ? ou une tabulation. Ce champ est obligatoire. Un pool d'adresses IP DHCP est une plage (ou pool) d'adresses IP disponibles que le switch peut affecter aux dispositifs connectés.
DHCP Pool Network	L'adresse IP du sous-réseau du pool d'adresses IP DHCP. Le format est une adresse numérique de 32 bits écrite sous forme de quatre nombres séparés par des points. Chaque nombre peut être compris entre 0 et 255. Ce champ est obligatoire.
Subnet Mask	L'adresse réseau qui identifie le sous-réseau (subnet) du pool d'adresses IP DHCP. Les sous-réseaux segmentent les dispositifs d'un réseau en plus petits groupes. La valeur par défaut est 255.255.255.0. Ce champ est obligatoire.
Starting IP	L'adresse IP de départ qui définit la plage d'adresses dans le pool d'adresses IP DHCP. Le format est une adresse numérique de 32 bits écrite sous forme de quatre nombres séparés par des points. Chaque nombre peut être compris entre 0 et 255. Assurez-vous qu'aucune des adresses IP que vous affectez n'est utilisée par un autre dispositif dans votre réseau. Ce champ est obligatoire.
Ending IP	L'adresse IP de fin qui définit la plage d'adresses dans le pool d'adresses IP DHCP. Le format est une adresse numérique de 32 bits écrite sous forme de quatre nombres séparés par des points. Chaque nombre peut être compris entre 0 et 255. Assurez-vous qu'aucune des adresses IP que vous affectez n'est utilisée par d'autres dispositifs sur votre réseau. Ce champ est obligatoire.
Default Router	L'adresse IP du routeur par défaut pour le client DHCP qui utilise ce serveur. Le format est une adresse numérique de 32 bits écrite sous forme de quatre nombres séparés par des points. Chaque nombre peut être compris entre 0 et 255.

Champ	Description
Domain Name	Le nom de domaine pour le client DHCP. Le nom peut compter jusqu'à 31 caractères alphanumériques. Le nom ne peut pas contenir un ? ou une tabulation.
DNS Server	Les adresses IP des serveurs IP d'un système de nom de domaine (DNS) disponibles pour un client DHCP. Le format est une adresse numérique de 32 bits écrite sous forme de quatre nombres séparés par des points. Chaque nombre peut être compris entre 0 et 255.
CIP Instance	Un nombre entre 1 et 15 pour identifier le pool d'adresses.
[Lease Length]	La durée du bail pour une adresse IP qui est affectée à un client DHCP. Cliquez sur l'une des options suivantes : • Never Expires (n'expire jamais) • User Defined (défini par l'utilisateur) Si vous cliquez sur User Defined, entrez la durée du bail en nombres de jours, d'heures et de minutes. Cette longueur de bail est utilisée pour toutes les affectations.

Réserver des adresses IP via la persistance DHCP

Vous pouvez réserver et préaffecter une adresse IP du pool d'adresses IP à un port de switch spécifique afin que des dispositifs connectés à ce port reçoivent toujours la même adresse IP, quelle que soit son adresse MAC.

La persistance DHCP est utile dans les réseaux qui sont configurés à l'avance, où il y a des dépendances sur les adresses IP exactes de certains dispositifs. Utilisez la persistance DHCP lorsque le dispositif connecté a un rôle spécifique à jouer et lorsque les autres dispositifs connaissent son adresse IP. Si le dispositif est remplacé, le dispositif de remplacement est assigné à la même adresse IP et les autres dispositifs du réseau ne requièrent aucune reconfiguration.

Lorsque la fonctionnalité de persistance DHCP est activée, le switch agit comme un serveur DHCP pour les autres dispositifs sur le même sous-réseau. Si le switch reçoit une demande de DHCP, il répond avec toutes les adresses IP non affectées dans son pool. Pour éviter cela, cochez la case Reserve Only dans la fenêtre DHCP. Cela empêche le switch de répondre lorsqu'il reçoit une demande.

Lorsque la persistance DHCP est activée sur un port et une demande de DHCP est faite à partir d'un dispositif connecté sur ce port, le switch affecte l'adresse IP à ce port dans la fenêtre DHCP. Il diffuse également la demande de DHCP pour le reste du réseau. Si un autre serveur DHCP avec des adresses disponibles est présent sur le réseau et reçoit cette demande, il peut essayer de répondre. Cela peut outrepasser l'adresse IP initiale affectée par le switch en fonction de la manière dont le dispositif se comporte (s'il prend la première réponse de l'adresse IP ou la dernière). Pour éviter que l'adresse IP ne soit substituée, activez la surveillance de trafic de DHCP sur le VLAN approprié. Cela bloque la diffusion de cette demande de DHCP, afin qu'aucun autre serveur, y compris un autre switch Stratix avec persistance DHCP activée, ne réponde.

Si vous utilisez la persistance DHCP, nous vous recommandons d'affecter au départ des adresses IP statiques aux dispositifs de fin. Si un dispositif de blocage échoue et est remplacé, la fonctionnalité de persistance DHCP affecte une adresse IP de la table de persistance DHCP. Le dispositif fonctionne correctement avec cette adresse IP, mais nous recommandons que vous réaffectiez une adresse IP statique aux dispositifs remplacés.

La figure et le tableau suivants illustrent les comportements de la persistance DHCP.

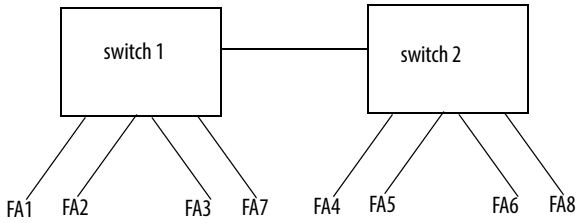


Tableau 12 - Comportement de la persistance DHCP

Si	Alors
• Le switch 1 a des ports FA1 à FA3 dans sa table de persistance • Le switch 2 a des ports FA4, FA5, FA6 et FA8 dans sa table de persistance • Reserve Only n'est pas sélectionné et DHCP Snooping est désactivé	Un nouveau dispositif connecté au switch 1 FA reçoit une adresse IP de la table de persistance du switch 1. Une demande de diffusion générale est également envoyée sur le réseau. Le switch 2 répond s'il y a une adresse non affectée dans son pool. Cela peut outrepasser l'affectation faite par le switch 1.
• Le switch 1 a des ports FA1 à FA3 dans sa table de persistance • Le switch 2 a des ports FA4, FA5, FA6 et FA8 dans sa table de persistance • Reserve Only est sélectionné sur les deux switchs et DHCP Snooping est désactivé	Un nouveau dispositif connecté au switch 1 FA reçoit une adresse IP de la table de persistance du switch 1. Une demande de diffusion générale est également envoyée sur le réseau. Le switch 2 ne répond pas à la demande. Notez que si le dispositif est connecté à FA7 du switch 1, il ne reçoit pas d'adresse IP provenant du pool de switchs, car il n'est pas défini dans la table de persistance et que les adresses inutilisées du pool sont bloquées.
• Le switch 1 a des ports FA1 à FA3 dans sa table de persistance • Le switch 2 a des ports FA4, FA5, FA6 et FA8 dans sa table de persistance • Réserve Only est sélectionné sur le switch 1 et DHCP snooping est désactivé, mais pas le switch 2 lorsque DHCP Snooping est désactivé	Un nouveau dispositif est connecté à FA1 et reçoit une adresse IP de la table de persistance. Une demande de diffusion générale est également envoyée sur le réseau. Le switch 2 ne répond pas à la demande. En outre, un dispositif connecté à FA4 reçoit une adresse IP de la table de persistance du switch 2. Une demande de diffusion générale est envoyée et le switch 1 répond avec une adresse IP inutilisée de son pool. Cela peut outrepasser le port affecté.
• Le switch 1 a des ports FA1 à FA3 dans sa table de persistance • Le switch 2 a des ports FA4, FA5, FA6 et FA8 dans sa table de persistance • DHCP Snooping est sélectionné • Reserved Only est coché	Un nouveau dispositif connecté au switch 1 FA reçoit une adresse IP de la table de persistance du switch 1. Aucune demande de diffusion générale n'est envoyée sur le réseau ; de ce fait, le switch 2 ne répond pas. Notez que si un dispositif est connecté à FA7 (indéfini dans la table de persistance DHCP) du switch 1, il ne reçoit pas d'adresse IP du pool de switchs, car il n'est pas défini dans la table de persistance et les adresses inutilisées dans le pool sont bloquées.
• Le switch 1 a des ports FA1 à FA3 dans sa table de persistance • Le switch 2 a des ports FA4, FA5, FA6 et FA8 dans sa table de persistance • DHCP Snooping est sélectionné • Reserved Only n'est pas coché	Un nouveau dispositif connecté au switch 1 FA reçoit une adresse IP de la table de persistance du switch 1. Aucune demande de diffusion générale n'est envoyée sur le réseau ; de ce fait, le switch 2 ne répond pas. Notez que si un dispositif est connecté à FA7 (indéfini dans la table de persistance DHCP) du switch 1, il reçoit une adresse IP non affectée du pool du switch 1.

Pour affecter, modifier ou supprimer une adresse IP de port de switch, cliquez sur l'onglet DHCP Persistance.

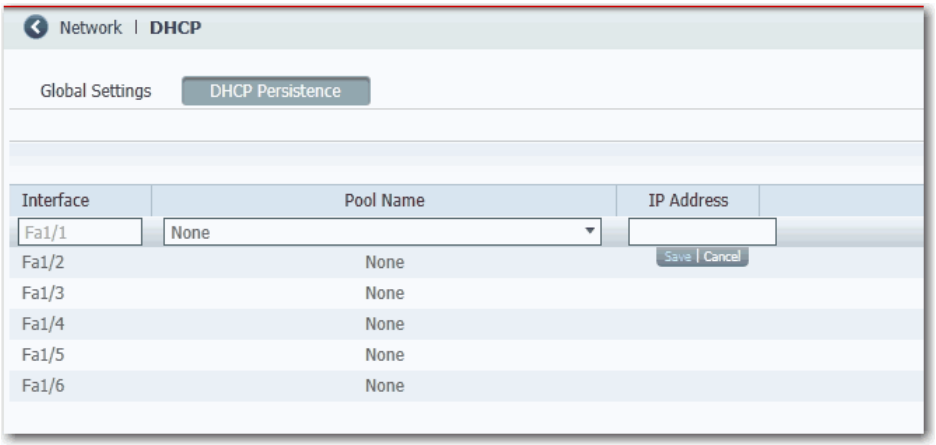


Tableau 13 - Champs de l'onglet DHCP Persistence

Champ	Description
Interface	Le numéro du port de switch, comprenant le type de port (Fa pour Fast Ethernet et Gi pour Gigabit Ethernet) et le numéro de port spécifique. Par exemple, FA1/1 est le port Fast Ethernet 1 sur le switch.
Pool Name	Le nom du pool d'adresses IP DHCP configuré sur le switch.
IP Address	L'adresse IP affectée au port du switch. L'adresse IP que vous affectez est réservée au port sélectionné et n'est pas disponible pour une affectation dynamique normale de DHCP. L'adresse IP doit être une adresse issue du pool spécifié dans le champ DHCP Pool Name.

Configuration des VLAN

Pour créer, modifier et supprimer des VLAN, dans le menu Configure, choisissez VLAN Management.

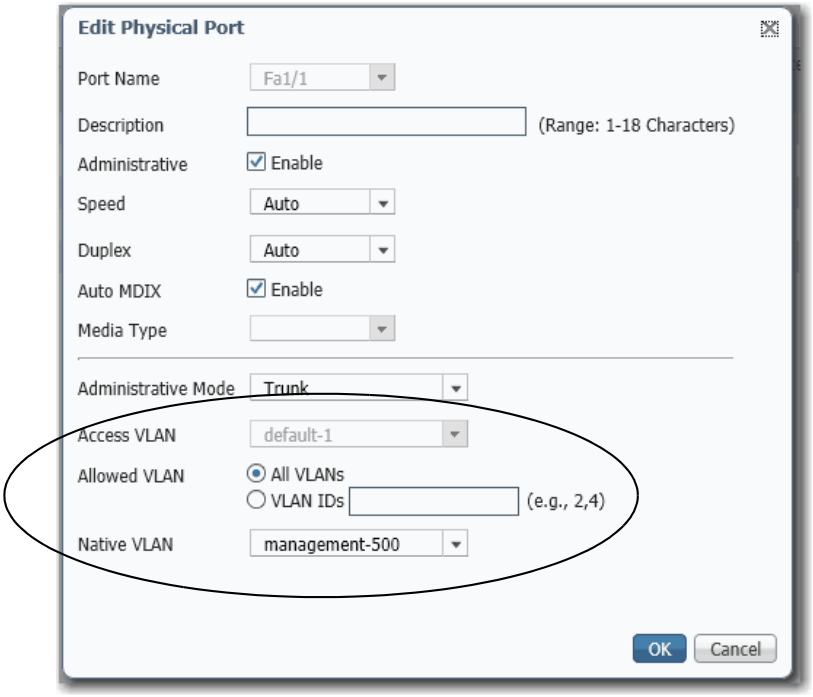
La valeur par défaut de VLAN ID est 1 et le nom pour le VLAN de gestion est default. Le VLAN par défaut seul peut être suffisant suivant la taille et les exigences de votre réseau. Nous vous recommandons de commencer par déterminer vos besoins en matière de VLAN avant de les créer.

Pour créer un VLAN, vous devez donner un nom et un numéro d'identification unique au VLAN. Vous pouvez modifier le nom d'un VLAN, mais pas son numéro. Vous ne pouvez pas modifier ou supprimer le VLAN par défaut.

Une fois que vous avez créé des VLAN, vous pouvez affecter des ports à ces VLAN. Avant d'affecter des ports aux VLAN, assurez-vous que chaque port a le rôle de port approprié.

Affecter des ports aux VLAN

Pour affecter des ports aux VLAN, utilisez la fenêtre Edit Physical Ports, tel que décrit à la page 109.



Configuration des ports PoE (Power over Ethernet)

Les fonctionnalités PoE et PoE+ sont prises en charge sur les switchs des ports PoE lorsqu'une alimentation adaptée est reliée au switch. Pour plus d'informations sur les exigences d'alimentation électrique, voir page 37.

Vous pouvez faire ce qui suit dans la fenêtre PoE :

- Limiter l'alimentation totale prise en charge.
- Configurer les réglages de mode et d'alimentation pour des ports individuels.

Pour la plupart des applications, la configuration par défaut (mode Auto) est suffisante et aucune configuration supplémentaire n'est nécessaire. Toutefois, vous pouvez personnaliser les réglages pour répondre à vos besoins. Par exemple, pour donner une priorité plus élevée d'alimentation au port PoE, réglez le mode sur Static et allouez la puissance à utiliser. Comme autre exemple, pour interdire les dispositifs requérant une puissance importante sur un port, réglez le mode sur Auto et spécifiez une limite de puissance maximale.

IMPORTANT Lorsque vous apportez des modifications de configuration PoE à un port, le port interrompt l'alimentation. La mise sous tension du port par la suite dépend de la nouvelle configuration, de l'état des autres ports PoE et de l'état du bilan d'alimentation.

Par exemple, si le port 1 est en mode Auto et dans l'état On, et que vous le configurez pour le mode Static, le switch supprime l'alimentation du port 1, détecte le dispositif alimenté et remet le port sous tension.

Si le port 1 est en mode Auto et dans l'état On, et que vous le configurez avec une puissance maximale de 10 W, le switch supprime l'alimentation à partir du port, puis redétecte le dispositif alimenté. Le switch remet sous tension le port seulement si le dispositif alimenté est un dispositif de Classe 1 ou Classe 2 ou un dispositif alimenté Cisco uniquement.

Pour configurer les ports PoE, dans le menu Configure, choisissez Power Management (gestion de l'alimentation).

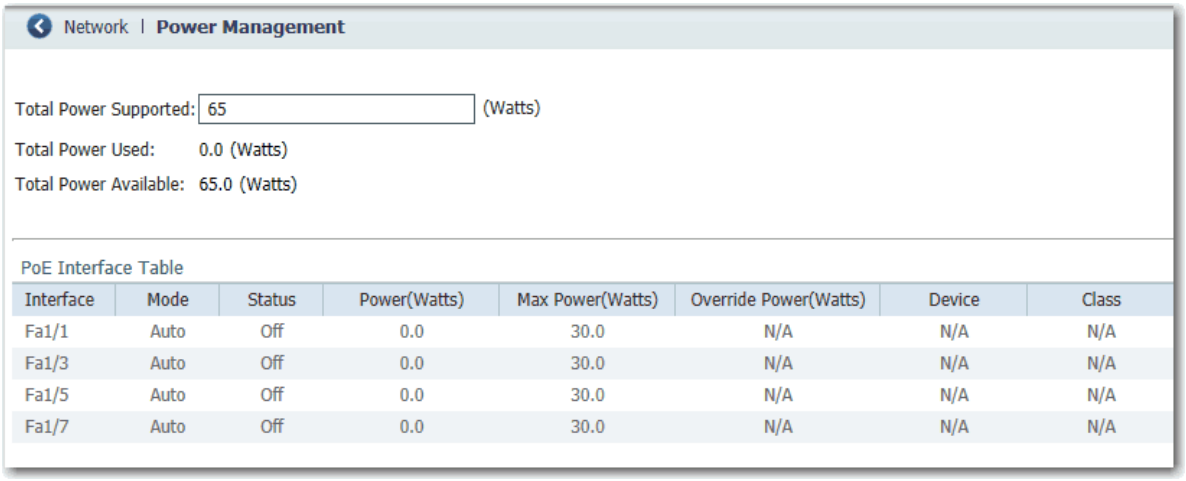


Tableau 14 - Champs de gestion de l'alimentation

Champ	Description
Total Power Supported (puissance totale prise en charge)	Pour limiter le budget de puissance totale PoE, saisissez une valeur appropriée selon la source d'alimentation : • Une source d'alimentation de 48 V prend en charge un maximum de 65 W. • Une source d'alimentation de 54 V prend en charge un maximum de 130 W. Lorsque vous enregistrez ce réglage, il modifie le budget de puissance totale PoE et réinitialise les dispositifs alimentés afin de répondre au nouveau budget. **IMPORTANT :** une discordance entre la puissance totale prise en charge et la source d'alimentation peut endommager le switch. Prenez soin de ne pas sursouscrire la source d'alimentation : • Si vous avez l'intention de relier le switch à une source d'alimentation qui permet plus de puissance que celle configurée, modifiez tout d'abord la source d'alimentation, puis spécifiez la puissance totale prise en charge. • Si vous avez l'intention de relier le switch à une source d'alimentation qui permet moins de puissance que celle configurée, modifiez tout d'abord la puissance totale prise en charge afin de définir une valeur appropriée, puis spécifiez la source d'alimentation.
Total Power Used (puissance totale utilisée)	Affiche la quantité de puissance que le module utilise actuellement.
Total Power Available (puissance totale disponible)	Affiche la quantité de puissance inutilisée disponible pour le module.
Interface	Affiche le numéro de port.
Mode	Affiche le mode de gestion de la puissance du port : • Auto : permet la détection de dispositifs alimentés et alloue automatiquement la puissance au port PoE si un dispositif est connecté. Ce réglage est sélectionné par défaut. Pour limiter la puissance utilisée par ce port, ajustez le réglage Max Power (puissance maxi.). • Static : réserve de la puissance pour ce port, même lorsqu'aucun dispositif n'est connecté, pour assurer que de la puissance est fournie lors de la détection de dispositifs. Vous pouvez également choisir le mode Static pour donner la priorité à un port. Le switch alloue la puissance aux ports en mode Static avant d'allouer la puissance aux ports en mode Auto. • Off : PoE est désactivé. Pour plus d'informations, voir Modes de gestion de l'alimentation à la page 67
Status (état)	Indique si PoE est activé (on) ou désactivé (off) sur le port.
Power (Watts)	Affiche la quantité de puissance allouée au port.
Max Power (Watts)	Affiche la quantité maximale de puissance disponible pour le port : Ports PoE : 4 à 15,4 W Ports PoE+ : 4 à 30 W
Override Power (Watts) (surpuissance)	Indique le surpassement de puissance configuré pour le port. Cette configuration surpasse à la fois la classification IEEE illustrée dans la colonne Class et la négociation de puissance. Si aucun surpassement n'est configuré, le champ affiche N/A. Vous ne pouvez configurer un surpassement de puissance qu'à l'aide de l'interface de ligne de commande (CLI). Pour plus d'informations, reportez-vous au Guide de configuration du logiciel Cisco IE 3000. **EXEMPLE :** un administrateur peut choisir de configurer un surpassement lorsque les besoins en puissance d'un dispositif connecté sont connus et sont inférieurs à la valeur maximale pour la classe. Par exemple, si un dispositif requiert 5 W uniquement, mais qu'il est en Classe 0, qui permet un maximum de 15,4 W, la configuration d'un surpassement permet de distribuer plus de puissance à d'autres dispositifs.
Device (dispositif)	Affiche le dispositif connecté au port. Si aucun dispositif n'est connecté au port, le champ affiche N/A.
Class	Affiche la classification de puissance du dispositif alimenté (PD). Pour plus d'informations sur les classifications de puissance, voir Tableau 4 à la page 66.

Configuration de la synchronisation temporelle PTP

La norme IEEE 1588 définit un protocole appelé protocole PTP (Precision Time Protocol) qui permet une synchronisation précise des horloges dans les systèmes de mesure et de commande. Les horloges communiquent les unes avec les autres sur le réseau de communication EtherNet/IP. Le protocole PTP permet à des systèmes hétérogènes qui comprennent des horloges de différentes précisions, résolutions et stabilités inhérentes de se synchroniser. Le protocole PTP génère une relation maître-esclave parmi les horloges du système. En définitive, toutes les horloges s'alignent sur l'heure d'une horloge sélectionnée comme étant l'horloge principale.

Par défaut, PTP est désactivé sur tous les ports Fast Ethernet et Gigabit Ethernet sur le switch.

Le switch prend en charge les modes Synchronization Clock suivants :

- **Mode End-to-End Transparente** : le switch synchronise en transparence toutes les horloges esclaves avec l'horloge maître reliée au switch.

  Le switch corrige le retard encouru par chaque paquet en passant par le switch (connu sous le nom de temps de résidence). Ce mode provoque moins d'accumulation d'erreurs que le mode Boundary.

  En mode End-to-End Transparente, tous les switchs sont activés par défaut.

- **Mode Boundary** : le switch devient l'horloge parente avec laquelle les autres dispositifs connectés au switch synchronisent leurs horloges internes.

  Le switch et les dispositifs connectés échangent constamment des messages de temporisation pour corriger l'écart temporel provoqué par les décalages d'horloge et les délais sur le réseau.

  Ce mode peut éliminer les effets des fluctuations de la latence. Les erreurs pouvant s'accumuler dans les topologies en cascade, utilisez ce mode pour les réseaux contenant moins de quatre couches de dispositifs en cascade.

  En mode Boundary, un ou plusieurs ports du switch peuvent être activés par PTP.

- **Mode Forward (par défaut)** : le trafic est réacheminé par le switch (tout en étant défini comme prioritaire par QoS) mais n'est pas influencé par le switch.

IMPORTANT	Lorsque les réglages de message de temporisation PTP sont modifiés, souvenez-vous que le système ne fonctionne pas correctement tant que tous les dispositifs du système n'ont pas les mêmes valeurs.

Pour configurer PTP, dans le menu Configure, choisissez PTP.

Une fois que vous choisissez un mode de fonctionnement, vous pouvez modifier les réglages de chaque port. Les paramètres dépendent du mode sélectionné. Vous pouvez configurer PTP port par port lorsque le switch est en mode Boundary ou en mode End-to-end Transparente.

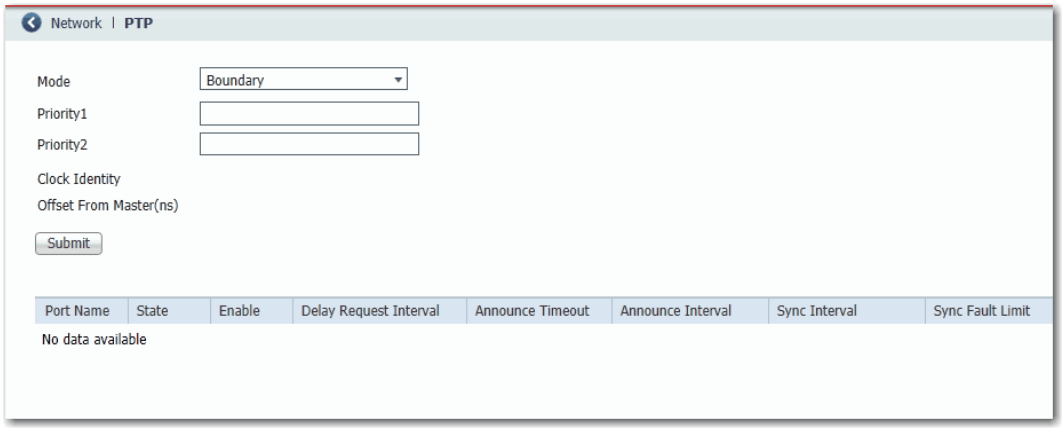


Tableau 15 - Champs PTP

Champ	Description
Mode	Choisissez un mode PTP : • Boundary : synchronise tous les ports du switch avec l'horloge Grandmaster en utilisant le mécanisme d'horloge IEEE 1588 V 2 Boundary. • End-to-End Transparente : calcule et ajoute le retard du switch au paquet PTP en utilisant le mécanisme d'horloge IEEE 1588 V2 End-to-End Transparente. Dans ce mode, tous les ports du switch sont activés par PTP. En mode Boundary, un ou plusieurs ports du switch peuvent être activés par PTP. Vous pouvez activer ou désactiver PTP port par port. • Forward (valeur par défaut) : fait passer les paquets PTP sans interférences.
Priority 1 (priorité 1)	Le switch utilisé pour outrepasser les critères par défaut, tels que la qualité ou la classe de l'horloge, pour la sélection de la meilleure horloge maître.
Priority 2 (priorité 2)	Le switch utilisé comme séparateur entre deux dispositifs qui sont sinon identiques au niveau des critères par défaut. Exemple : vous pouvez donner la priorité à un switch spécifique sur d'autres switchs identiques. La plage est entre 0 et 255. Une valeur inférieure a la priorité. La valeur par défaut est 128.
Clock Identity (identité d'horloge)	La source de l'horloge.
Offset from Master (ns) (décalage par rapport au maître)	La précision en nanosecondes à partir de l'horloge Grandmaster.
Port Name (nom de port)	Le numéro du port de switch, comprenant le type de port (Fa pour Fast Ethernet et Gi pour Gigabit Ethernet), le numéro du switch de base (1) et le numéro de port spécifique. Par exemple : FA1/1 est le port Fast Ethernet 1 sur le switch de base.
State (état)	(mode Boundary uniquement). L'état de synchronisation sur le port de switch avec l'horloge parente ou Grandmaster : • Listening : le port du switch est en attente pendant qu'une horloge parente ou Grandmaster est sélectionnée. • Pre-master : le port du switch est en transition pour passer à l'état Master. • Master : le switch agit comme une horloge parente pour les dispositifs connectés à ce port de switch. • Passive : le switch a détecté un chemin redondant vers une horloge parente ou Grandmaster. Par exemple, deux ports de switch différents revendiquent la même horloge parente ou Grandmaster. Pour éviter une boucle dans le réseau, l'un des ports passe à l'état Passive. • Uncalibrated : le port du switch ne peut pas se synchroniser avec l'horloge parente ou Grandmaster. • Slave : le port du switch est connecté à l'horloge parente ou Grandmaster, et en cours de synchronisation avec celle-ci. • Faulty : PTP ne fonctionne pas correctement sur ce port de switch. • Disabled : PTP n'est pas activé sur le port de switch.
Enable (validé)	Lorsqu'au moins un port de switch est activé par PTP, le mode Forward est sélectionné par défaut : Vous pouvez activer ou désactiver PTP port par port.

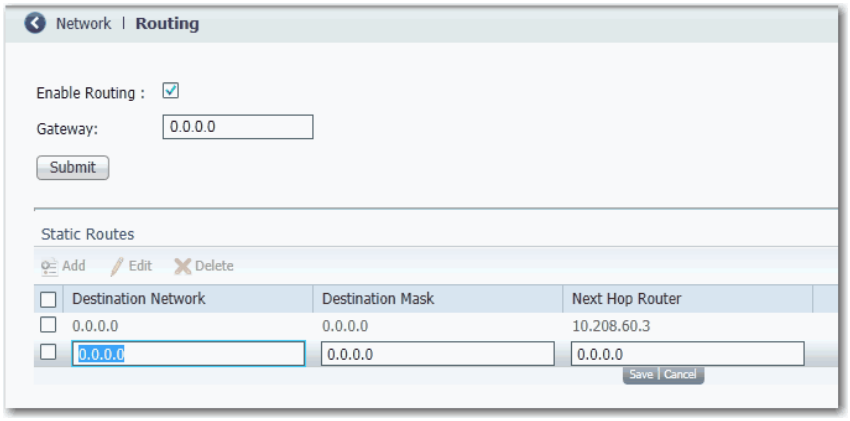
Tableau 15 - Champs PTP (suite)

Champ	Description
Delay Request Interval (intervalle de requête de délai)	L'intervalle de temps recommandé aux dispositifs connectés pour envoyer des messages de requête de délai lorsque le port du switch se trouve en état Master : • **-1** signifie une demi-seconde • **0** signifie 1 seconde • **1** signifie 2 secondes • **2** signifie 4 secondes • **3** signifie 8 secondes • **4** signifie 16 secondes • **5** signifie 32 secondes • **6** signifie 64 secondes La valeur par défaut est 5 (32 secondes).
Announce Timeout (timeout d'annonce)	Le nombre d'intervalles d'annonces devant s'écouler sans réception d'un message d'annonce envoyé par l'horloge Grandmaster avant que le switch ne sélectionne une nouvelle horloge Grandmaster. Le nombre peut être entre 2 et 10. La valeur par défaut est 3.
Announce Interval (intervalle d'annonce)	L'intervalle de temps pour l'envoi des messages d'annonce : • **0** signifie 1 seconde • **1** signifie 2 secondes • **2** signifie 4 secondes • **3** signifie 8 secondes • **4** signifie 16 secondes La valeur par défaut est 1 (2 secondes).
Sync Interval (intervalle de synchronisation)	L'intervalle de temps pour l'envoi de messages de synchronisation : • **-1** signifie une demi-seconde • **0** signifie 1 seconde • **1** signifie 2 secondes La valeur par défaut est 0 (1 seconde).
Sync Fault Limit (limite de défaut de synchronisation)	Le décalage d'horloge maximum avant que PTP ne tente de récupérer la synchronisation. La valeur peut être entre 50 et 500 000 000 nanosecondes. La valeur par défaut est 50 000 nanosecondes. Nous vous déconseillons de définir la limite de synchronisation en dessous de la valeur par défaut (50 000 nanosecondes). Utilisez les valeurs inférieures à 50 000 nanosecondes uniquement dans les réseaux ayant une horloge Grandmaster de très haute précision. Dans ces réseaux, il est essentiel que les dispositifs très sensibles restent synchronisés.

Activation et configuration du routage

Avant d'activer le routage , vous devez réaffecter de la mémoire du switch pour le routage, comme décrit à la page 156.

Pour activer le routage, dans le menu Configure, choisissez Routing (routage).



Dans la fenêtre Routing, vous pouvez activer le routage connecté uniquement ou le routage statique et connecté. Une fois le routage statique activé, le routage connecté est activé par défaut. Pour plus d'informations sur ces types de routage, reportez-vous à Routage à la page 92.

Activer le routage connecté uniquement

Pour activer le routage connecté uniquement, cochez Enable Routing (valider le routage), puis cliquez sur Submit (soumettre).

Aucune configuration supplémentaire n'est requise pour le routage connecté.

Activer le routage statique et connecté

Pour activer le routage statique et connecté, suivez les étapes ci-après.

1. Cochez Enable Routing (valider le routage), puis cliquez sur Submit (soumettre).
2. Configurez les informations de routage statique telles que décrites ci-dessous.

Champ	Description
Destination Network (réseau de destination)	L'adresse IP de destination.
Destination Mask (masque de destination)	Le masque de sous-réseau de destination.
Next Hop Router (prochain saut de routeur)	L'adresse IP du routeur où ce switch va envoyer les paquets pour la destination spécifiée.

Configuration de STP

Les modes STP (Spanning Tree Protocol) sont les suivants :

- Multiple Spanning Tree (MST) empêche les boucles de réseau en activant uniquement un chemin actif pour le trafic. MST fournit également un chemin redondant si le chemin d'accès actif n'est plus disponible. Il s'agit du mode par défaut.
- Per VLAN Spanning Tree Plus (PVST+) s'exécute sur chaque VLAN du switch jusqu'au maximum pris en charge, assurant un chemin sans boucle à travers le réseau.
- Rapid Per VLAN Spanning Tree Plus (RPVST+) supprime immédiatement de façon dynamique les entrées d'adresse MAC apprises sur réception d'un changement de topologie. Par contraste, PVST+ utilise un temps de vieillissement court pour les adresses MAC dynamiquement apprises.

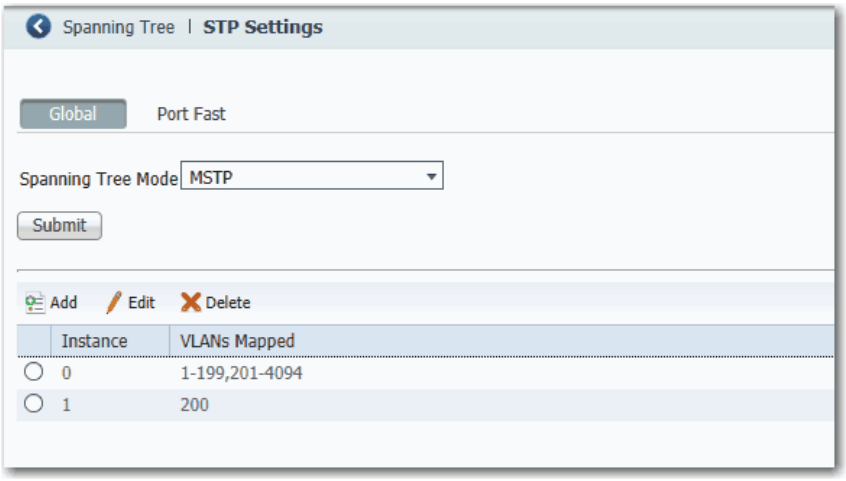
Nous vous recommandons de laisser STP activé pour éviter les boucles de réseau et fournir un chemin redondant si le chemin d'accès actif n'est plus disponible.

IMPORTANT La désactivation de STP peut affecter la connectivité avec le réseau.

Pour configurer les réglages de Spanning Tree Protocol, dans le menu Configure, choisissez STP.

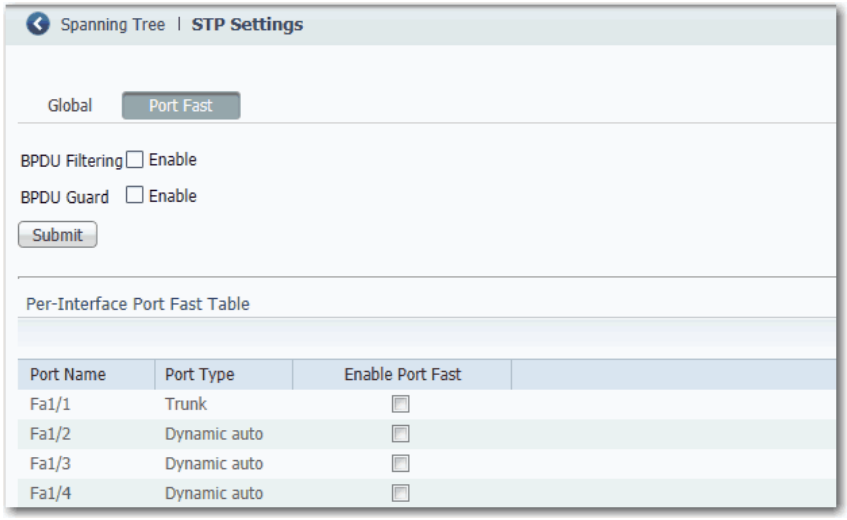
Réglages globaux

Pour choisir le mode STP du switch ou configurer STP sur des VLAN individuels, cliquez sur l'onglet Global. Sur l'onglet Global, vous pouvez ajouter, modifier ou supprimer des instances. Si vous choisissez le mode PVST+ ou Rapid PVST+, vous pouvez activer ou désactiver STP sur chaque instance.



Réglages PortFast

Pour activer PortFast et les fonctionnalités connexes, cliquez sur l'onglet PortFast. Sur l'onglet PortFast, vous pouvez modifier la manière dont STP est mis en œuvre sur les ports individuels.



Les fonctionnalités PortFast sont généralement activées uniquement sur les ports d'accès qui se connectent aux dispositifs, tels que les ordinateurs personnels, les points d'accès et les serveurs, qui ne sont pas censés envoyer des unités de données de protocole de pont (BPDU). Ces fonctionnalités ne sont généralement pas activées sur les ports qui se connectent à des switchs, car des boucles d'arbre maximal pourraient se produire.

Fonctionnalités BPDU

Les switchs échangent des trames spéciales appelées BPDU afin de communiquer des informations sur le réseau, de suivre les changements et de créer la topologie STP. Comme les informations de BPDU transmises révèlent des informations de réseau et les BPDU reçues peuvent influencer votre topologie STP, il peut être intéressant d'activer BPDU Filtering et BPDU Guard sur vos ports d'accès. Ces fonctionnalités empêchent un dispositif indésirable d'interférer avec votre topologie STP. Cependant, nous vous recommandons d'utiliser les fonctionnalités ci-après avec précaution :

- BPDU Filtering : cette fonctionnalité PortFast bloque tout envoi et toute réception de BPDU via l'ensemble des ports activés PortFast. Cette fonctionnalité désactive STP sur ces ports et peut entraîner des boucles. Si une BPDU est reçue, PortFast est désactivé sur le port et les réglages STP globaux sont appliqués. Pour activer BPDU Filtering sur tous les ports sur lesquels PortFast est activé, cochez Enable (valider).

- BPDU Guard : cette fonctionnalité PortFast arrête un port s'il reçoit une BPDU. Pour activer BPDU Guard sur tous les ports sur lesquels PortFast est activé, cochez Enable (valider).

Notez que si vous activez ces deux fonctionnalités, BPDU Guard n'a aucun effet car BPDU Filtering empêche le port de recevoir toute BPDU.

Par tableau d'interface PortFast Table

L'arbre maximal exige qu'une interface progresse à travers les états d'écoute et d'apprentissage, pour échanger des informations et établir un chemin sans boucle avant de pouvoir réacheminer des trames. Sur les ports qui se connectent aux dispositifs tels que les stations de travail et les serveurs, vous pouvez autoriser une connexion immédiate. PortFast fait immédiatement passer le port en mode de réacheminement STP sur réception du message d'établissement de liaison.

Pour activer PortFast sur une interface et appliquer les fonctionnalités BPDU sélectionnées à l'interface, sélectionnez l'interface, puis cochez Enable Port Fast (valider PortFast).

Configuration de REP

Pour configurer REP (Resilient Ethernet Protocol), dans le menu Configure, choisissez REP.

Pour créer un segment REP, définissez un ID de segment et un type de port sur les ports désirés.

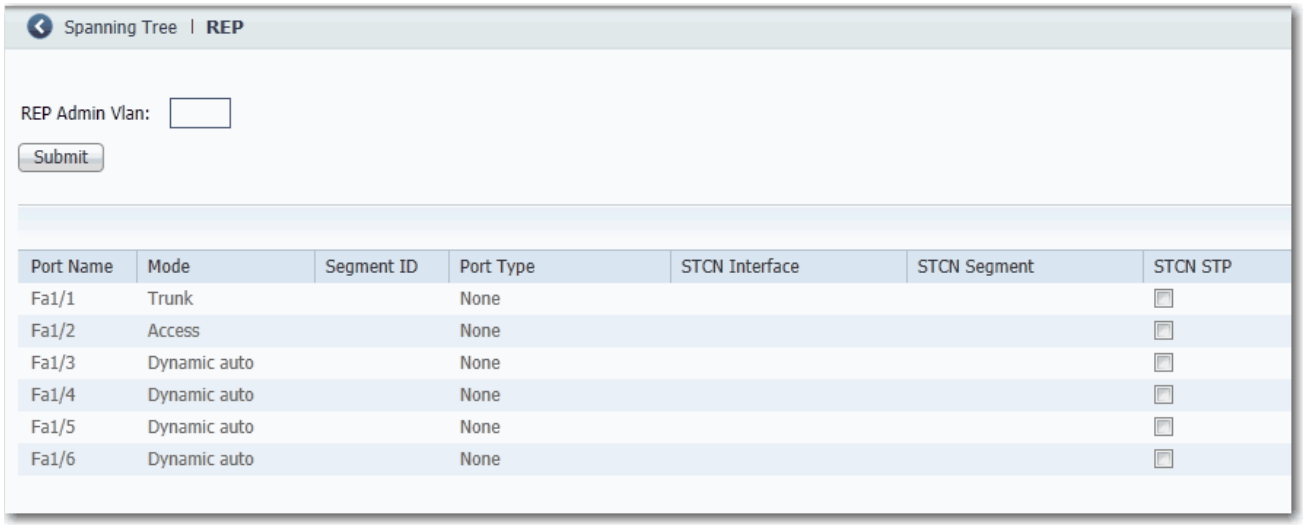


Tableau 16 - Champs REP

Champ	Description
REP Admin VLAN	Le VLAN administratif. La plage est entre 2 et 4 094. La valeur par défaut est VLAN 1. Les ports REP sont affectés au même REP Admin VLAN. Si le REP Admin VLAN change, tous les ports REP sont automatiquement affectés au nouveau REP Admin VLAN.
Port Name (nom de port)	Le numéro du port de switch, comprenant le type de port (Fa pour Fast Ethernet et Gi pour Gigabit Ethernet).
Mode	Le mode administratif. Pour définir ce mode, dans le menu Configure, choisissez Port Settings (réglages de port).
Segment ID (ID de segment)	L'ID du segment. La plage d'ID de segment est entre 1 et 1 024. Si aucune ID de segment n'est définie, REP est désactivé.
Port Type (type de port)	Chaque segment REP doit avoir exactement deux ports frontaux principaux et peut avoir des ports secondaires à utiliser lorsqu'un port principal échoue. Vous pouvez spécifier les ports principaux et secondaires préférés. Le fait de configurer un port comme le favori ne garantit pas qu'il deviendra le port alternatif, mais lui donne un léger avantage sur les autres. Vous pouvez également indiquer qu'un port est connecté à des switchs qui ne prennent pas en charge le REP. Choisissez l'un des types ci-après : • Edge : un port frontal secondaire qui participe à l'équilibrage de la charge VLAN. • Edge no-neighbor : un port frontal secondaire qui est connecté à un switch non-REP. • Edge no-neighbor preferred : un port frontal secondaire qui est connecté à un switch non-REP et est le port alternatif préféré pour l'équilibrage de la charge VLAN. • Edge no-neighbor primary : un port frontal secondaire qui participe toujours dans l'équilibrage de la charge VLAN dans ce segment REP et est connecté à un switch non-REP. • Edge no-neighbor primary preferred : un port frontal secondaire qui participe toujours dans l'équilibrage de la charge VLAN dans ce segment REP, est connecté à un switch non-REP et est le port préféré pour l'équilibrage de la charge VLAN. • Edge preferred : un port frontal secondaire qui est le port alternatif préféré pour l'équilibrage de la charge VLAN. • Edge primary : un port frontal qui participe toujours dans l'équilibrage de la charge VLAN dans ce segment REP. • Edge primary preferred : un port frontal qui participe toujours dans l'équilibrage de la charge VLAN dans ce segment REP et est le port préféré pour l'équilibrage de la charge VLAN. • None : ce port ne fait pas partie du segment REP. La valeur par défaut est None (aucun). • Preferred : un port frontal secondaire qui est le port alternatif préféré pour l'équilibrage de la charge VLAN.
STCN Interface	Configure les notifications de changement de topologie de segment (STCN) pour un port. La valeur par défaut est None (aucune). Les TCN sont utilisés au sein du segment pour notifier les voisins REP des modifications de topologie. En front de segment, REP peut propager la notification vers le STP, ou vers d'autres segments REP.
STCN Segment	Configure des STCN vers un ID de segment. La valeur par défaut est un champ vide. Les TCN sont utilisés au sein du segment pour notifier les voisins REP des modifications de topologie. En front de segment, REP peut propager la notification vers le STP, ou vers d'autres segments REP.
STCN STP	Configure des STCN vers un réseau STP. La valeur par défaut est une case décochée. Les TCN sont utilisés au sein du segment pour notifier les voisins REP des modifications de topologie. En front de segment, REP peut propager la notification vers le STP, ou vers d'autres segments REP.

Configuration de NAT

Pour configurer NAT, suivez l'une des procédures ci-dessous, en fonction de votre application :

- Créer des instances NAT pour le trafic acheminé via un switch de couche 3 ou un routeur

  Pour un exemple de cette application, consultez Figure 4 à la page 82.
- Créer des Instances NAT pour le trafic acheminé via un switch de Couche 2

  Pour un exemple de cette application, consultez Figure 5 à la page 82.

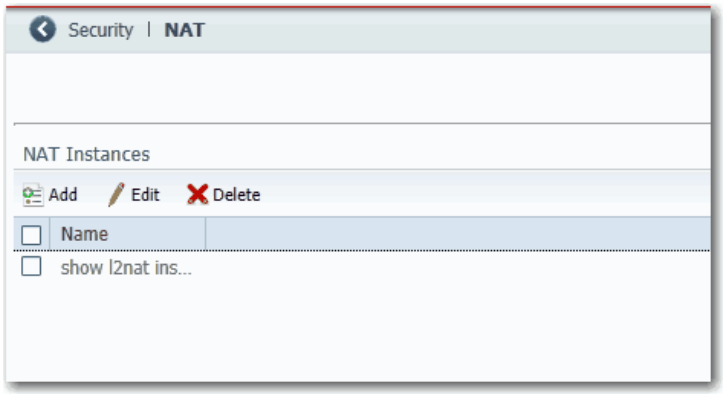
IMPORTANT	Mettez en place tous les rôles Smartport et VLAN avant de créer des instances NAT. Si vous modifiez un rôle de smartport ou le VLAN natif pour un port associé à une instance NAT, vous devez réaffecter les VLAN à l'instance NAT.

IMPORTANT	À la suite d'un transfert de Couche 2, les sessions de trafic en cours restent maintenues jusqu'à la déconnexion manuelle. Si vous modifiez une traduction existante, vous devez déconnecter manuellement les sessions de trafic associées à toutes les séances pour que la nouvelle traduction puisse être effective.

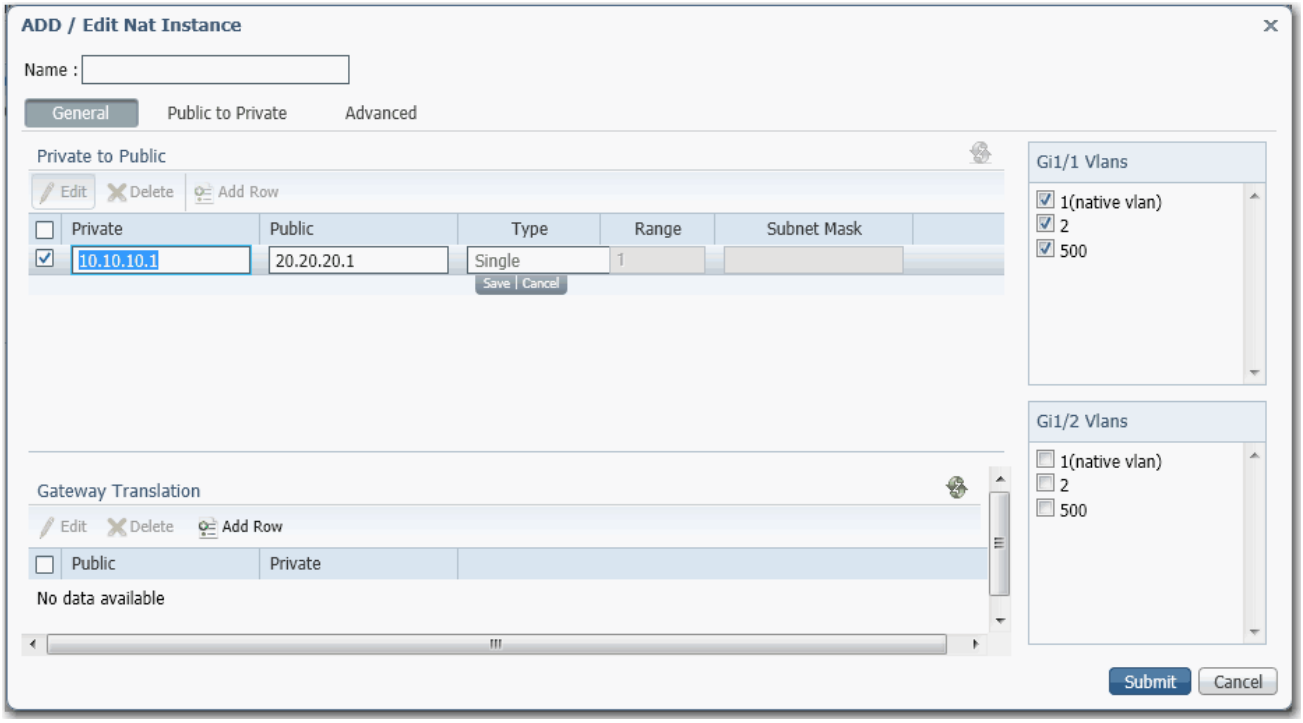
Créer des instances NAT pour le trafic acheminé via un switch de couche 3 ou un routeur

Pour créer une instance NAT pour le trafic acheminé via un switch de couche 3 ou un routeur, suivez les étapes ci-après.

1. Dans le menu Configure, choisissez NAT pour afficher la fenêtre NAT.



2. Cliquez sur Add (ajouter) pour afficher l'onglet General de la fenêtre Add/Edit NAT Instance (ajouter/modifier une instance NAT).



3. Dans le champ Name (nom), saisissez un nom unique pour identifier l'instance.

   Le nom de l'instance ne peut pas inclure d'espaces ni dépasser 32 caractères.

4. À partir de la liste des VLAN sur la droite, cochez la case en regard de chaque VLAN à affecter à l'instance.

   Pour plus d'informations sur les affectations VLAN, voir page 83.

5. Dans la zone Private to Public (prive à public), cliquez sur Add Row (ajouter une rangée), renseignez les champs, puis cliquez sur Save (enregistrer).

<table>
<tr><th>Champ</th><th colspan="2">Description</th></tr>
<tr><td>Private IP Address (adresse IP privée)</td><td colspan="2">Saisissez une adresse IP privée :
• Pour traduire une seule adresse, saisissez l'adresse existante pour le dispositif sur le sous-réseau privé.
• Pour traduire une plage d'adresses, saisissez la première adresse dans la plage d'adresses séquentielles.
• Pour traduire des adresses dans un sous-réseau, saisissez l'adresse de départ actuelle d'un dispositif sur le sous-réseau privé. Cette adresse doit correspondre à la taille du masque de sous-réseau à traduire comme illustré ci-dessous.</td></tr>
<tr><td></td><td>Masque de sous-réseau</td><td>Adresse de départ du sous-réseau privé</td></tr>
<tr><td></td><td>255.255.0.0</td><td>Les deux derniers octets doivent se terminer par 0.
EXEMPLE : 192.168.0.0</td></tr>
<tr><td></td><td>255.255.255.0</td><td>Le dernier octet doit se terminer par 0.
EXEMPLE : 192.168.1.0</td></tr>
<tr><td></td><td>255.255.255.128</td><td>Le dernier octet doit se terminer par 0 ou 128.
EXEMPLE : 192.168.1.0 ou 192.168.1.128</td></tr>
<tr><td></td><td>255.255.255.192</td><td>Le dernier octet doit correspondre à l'une des valeurs suivantes : 0, 64, 128, 192.
EXEMPLE : 192.168.1.64</td></tr>
<tr><td></td><td>255.255.255.224</td><td>Le dernier octet doit correspondre à l'une des valeurs suivantes : 0, 32, 64, 96, 128, 160, 192, 224.
EXEMPLE : 192.168.1.32</td></tr>
<tr><td></td><td>255.255.255.240</td><td>Le dernier octet doit correspondre à l'une des valeurs suivantes : 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240.
EXEMPLE : 192.168.1.16</td></tr>
</table>

<table>
<tr><th>Champ</th><th>Description</th></tr>
<tr><td>Public IP Address (adresse IP publique)</td><td>Saisissez une adresse IP publique :
• Pour traduire une seule adresse, saisissez une adresse publique unique pour représenter le dispositif.
• Pour traduire une plage d'adresses, saisissez la première adresse dans la plage d'adresses séquentielles.
• Pour traduire des adresses dans un sous-réseau, saisissez une adresse publique de départ unique pour représenter les dispositifs. Cette adresse doit correspondre à la taille du masque de sous-réseau à traduire comme illustré ci-dessous.
<table>
<tr><th>Masque de sous-réseau</th><th>Adresse de départ du sous-réseau public</th></tr>
<tr><td>255.255.0.0</td><td>Les deux derniers octets doivent se terminer par 0.
EXEMPLE : 10.200.0.0</td></tr>
<tr><td>255.255.255.0</td><td>Le dernier octet doit se terminer par 0.
EXEMPLE : 10.200.1.0.</td></tr>
<tr><td>255.255.255.128</td><td>Le dernier octet doit se terminer par 0 ou 128.
EXEMPLE : 10.200.1.0 ou 10.200.1.128</td></tr>
<tr><td>255.255.255.192</td><td>Le dernier octet doit correspondre à l'une des valeurs suivantes : 0, 64, 128, 192.
EXEMPLE : 10.200.1.64</td></tr>
<tr><td>255.255.255.224</td><td>Le dernier octet doit correspondre à l'une des valeurs suivantes : 0, 32, 64, 96, 128, 160, 192, 224.
EXEMPLE : 10.200.1.32</td></tr>
<tr><td>255.255.255.240</td><td>Le dernier octet doit correspondre à l'une des valeurs suivantes : 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240.
EXEMPLE : 10.200.1.16</td></tr>
</table></td></tr>
<tr><td>Type</td><td>Choisissez l'une des valeurs ci-après :
• Single : traduire une seule adresse.
• Range : traduire une plage d'adresses.
• Subnet : traduire toutes les adresses dans le sous-réseau privé ou une partie du sous-réseau privé.</td></tr>
<tr><td>Range (plage)</td><td>Saisissez le nombre d'adresses à traduire. Ce champ est disponible uniquement si vous choisissez Range (plage) dans le champ Type.
Valeurs valables : 1 à 128
Valeur par défaut = 1
IMPORTANT : chaque adresse dans la plage compte comme une entrée de traduction. Le switch prend en charge un maximum de 128 saisies de traduction.</td></tr>
<tr><td>Subnet Mask (masque de sous-réseau)</td><td>Saisissez le masque de sous-réseau pour les adresses à traduire.
Valeurs valables :
• Classe B : 255.255.0.0
• Classe C : 255.255.255.0
• Portion de Classe C :
– 255 255 255 128 (fournit 128 adresses par entrée de traduction)
– 255 255 255 192 (fournit 64 adresses par entrée de traduction)
– 255 255 255 224 (fournit 32 adresses par entrée de traduction)
– 255.255.255.240 (fournit 16 adresses par entrée de traduction)</td></tr>
</table>

6. Dans la zone Gateway Translation, cliquez sur Add Row (ajouter une rangée), renseignez les champs, puis cliquez sur Save (enregistrer).

   La traduction de passerelle permet aux dispositifs du sous-réseau public de communiquer avec les dispositifs du sous-réseau privé.

Champ	Description
Public	Saisissez l'adresse de la passerelle par défaut du switch ou routeur de couche 3 connecté au port de liaison montante du switch.
Private (privé)	Tapez une adresse IP unique pour représenter le switch Couche 3 ou le routeur sur le réseau privé.

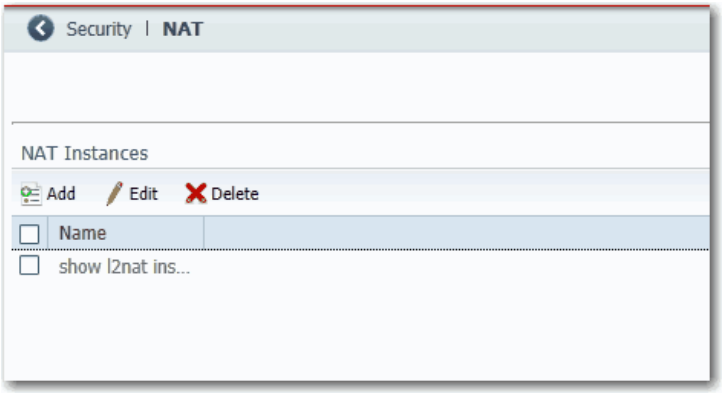
7. (facultatif). Pour configurer les autorisations de trafic et les corrections des paquets, poursuivez au paragraphe Configuration des permis et des corrections de trafic à la page 136.

8. Cliquez sur Submit (soumettre).

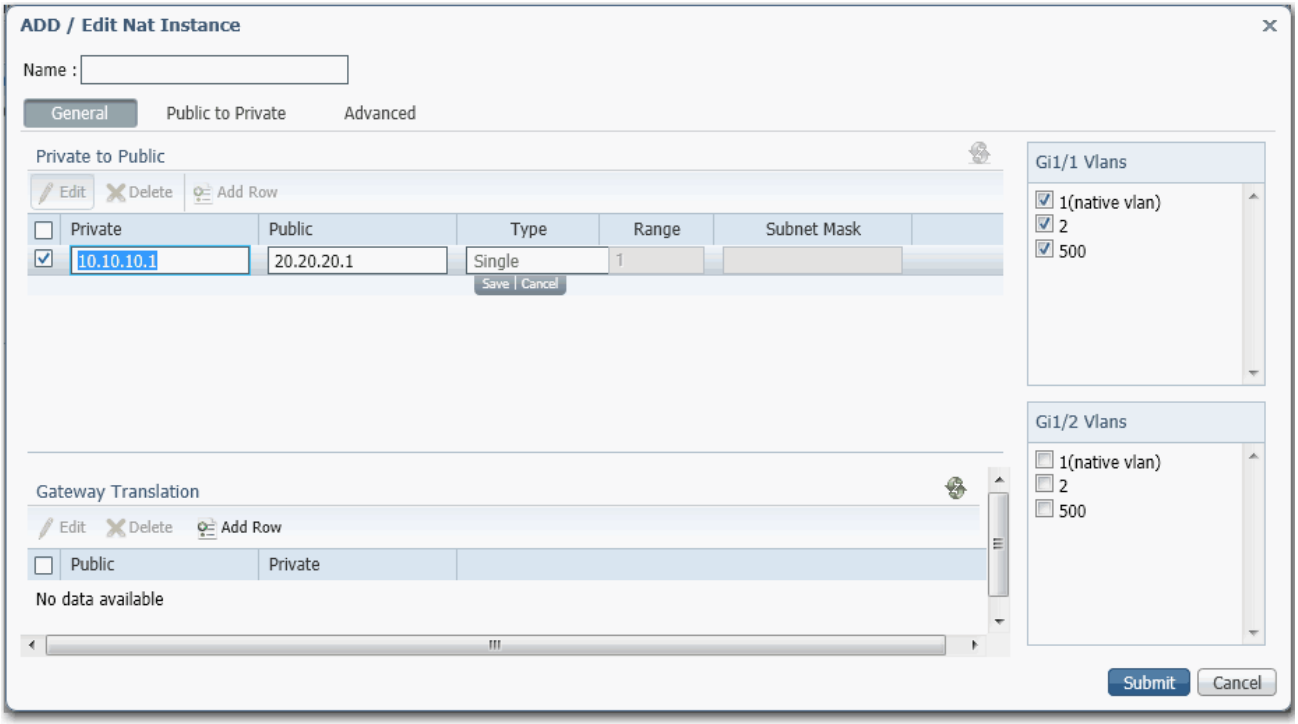
Créer des Instances NAT pour le trafic acheminé via un switch de Couche 2

Pour créer une instance NAT pour le trafic acheminé via un switch de Couche 2, suivez ces étapes.

1. Dans le menu Configure, choisissez NAT pour afficher la fenêtre NAT.



2. Cliquez sur Add (ajouter) pour afficher l'onglet General de la fenêtre Add/Edit NAT Instance (ajouter/modifier une instance NAT).



3. Dans le champ Name (nom), saisissez un nom unique pour identifier l'instance.

   Le nom de l'instance ne peut pas inclure d'espaces ni dépasser 32 caractères.

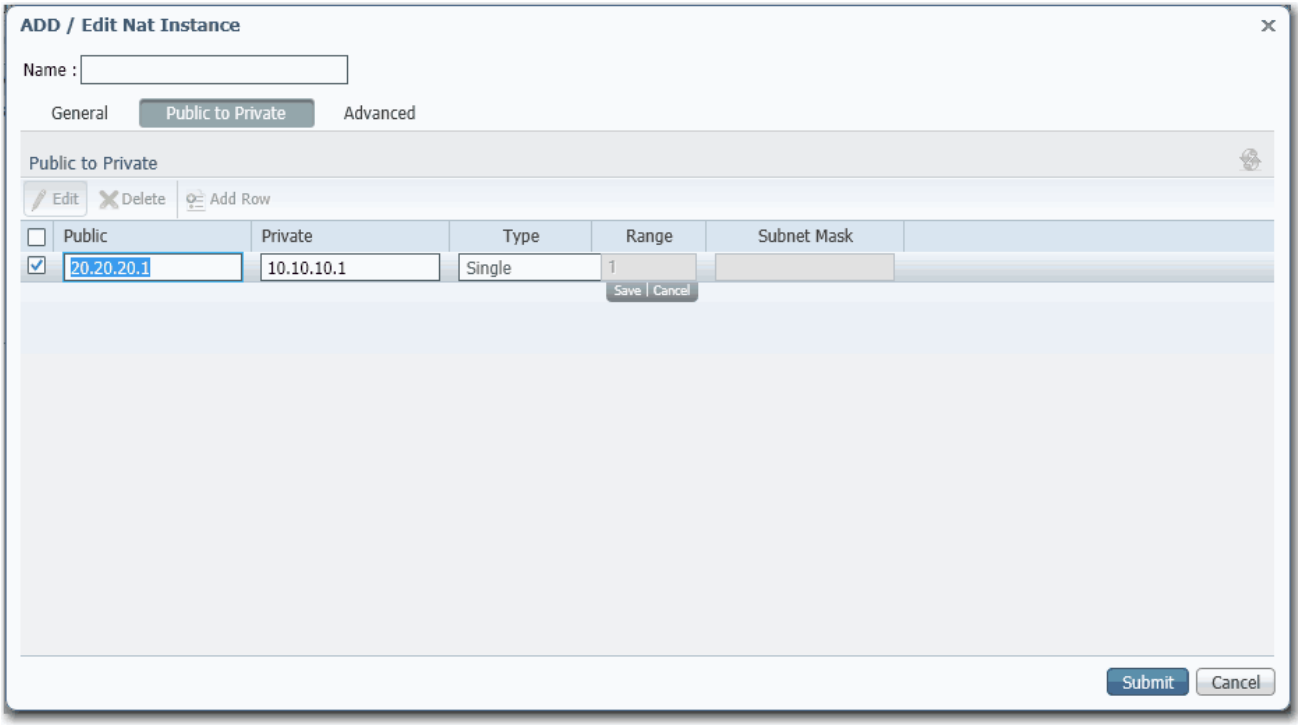
4. À partir de la liste des VLAN sur la droite, cochez la case en regard de chaque VLAN à affecter à l'instance.

   Pour plus d'informations sur les affectations VLAN, voir page 83.

5. Dans la zone Private to Public (prive à public), cliquez sur Add Row (ajouter une rangée), renseignez les champs, puis cliquez sur Save (enregistrer).

<table>
<tr><th>Champ</th><th colspan="2">Description</th></tr>
<tr><td>Private IP Address (adresse IP privée)</td><td colspan="2">Saisissez une adresse IP privée :
• Pour traduire une seule adresse, saisissez l'adresse existante pour le dispositif sur le sous-réseau privé.
• Pour traduire une plage d'adresses, saisissez la première adresse dans la plage d'adresses séquentielles.
• Pour traduire des adresses dans un sous-réseau, saisissez l'adresse de départ actuelle d'un dispositif sur le sous-réseau privé. Cette adresse doit correspondre à la taille du masque de sous-réseau à traduire comme illustré ci-dessous.</td></tr>
<tr><td></td><td>Masque de sous-réseau</td><td>Adresse de départ du sous-réseau privé</td></tr>
<tr><td></td><td>255.255.0.0</td><td>Les deux derniers octets doivent se terminer par 0.
EXEMPLE : 192.168.0.0</td></tr>
<tr><td></td><td>255.255.255.0</td><td>Le dernier octet doit se terminer par 0.
EXEMPLE : 192.168.1.0</td></tr>
<tr><td></td><td>255.255.255.128</td><td>Le dernier octet doit se terminer par 0 ou 128.
EXEMPLE : 192.168.1.0 ou 192.168.1.128</td></tr>
<tr><td></td><td>255.255.255.192</td><td>Le dernier octet doit correspondre à l'une des valeurs suivantes : 0, 64, 128, 192.
EXEMPLE : 192.168.1.64</td></tr>
<tr><td></td><td>255.255.255.224</td><td>Le dernier octet doit correspondre à l'une des valeurs suivantes : 0, 32, 64, 96, 128, 160, 192, 224.
EXEMPLE : 192.168.1.32</td></tr>
<tr><td></td><td>255.255.255.240</td><td>Le dernier octet doit correspondre à l'une des valeurs suivantes : 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240.
EXEMPLE : 192.168.1.16</td></tr>
<tr><td>Public IP Address (adresse IP publique)</td><td colspan="2">Saisissez une adresse IP publique :
• Pour traduire une seule adresse, saisissez une adresse publique unique pour représenter le dispositif.
• Pour traduire une plage d'adresses, saisissez la première adresse dans la plage d'adresses séquentielles.
• Pour traduire des adresses dans un sous-réseau, saisissez une adresse publique de départ unique pour représenter les dispositifs. Cette adresse doit correspondre à la taille du masque de sous-réseau à traduire comme illustré ci-dessous.</td></tr>
<tr><td></td><td>Masque de sous-réseau</td><td>Adresse de départ du sous-réseau public</td></tr>
<tr><td></td><td>255.255.0.0</td><td>Les deux derniers octets doivent se terminer par 0.
EXEMPLE : 10.200.0.0</td></tr>
<tr><td></td><td>255.255.255.0</td><td>Le dernier octet doit se terminer par 0.
EXEMPLE : 10.200.1.0.</td></tr>
<tr><td></td><td>255.255.255.128</td><td>Le dernier octet doit se terminer par 0 ou 128.
EXEMPLE : 10.200.1.0 ou 10.200.1.128</td></tr>
<tr><td></td><td>255.255.255.192</td><td>Le dernier octet doit correspondre à l'une des valeurs suivantes : 0, 64, 128, 192.
EXEMPLE : 10.200.1.64</td></tr>
<tr><td></td><td>255.255.255.224</td><td>Le dernier octet doit correspondre à l'une des valeurs suivantes : 0, 32, 64, 96, 128, 160, 192, 224.
EXEMPLE : 10.200.1.32</td></tr>
<tr><td></td><td>255.255.255.240</td><td>Le dernier octet doit correspondre à l'une des valeurs suivantes : 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240.
EXEMPLE : 10.200.1.16</td></tr>
<tr><td>Type</td><td colspan="2">Choisissez l'une des valeurs ci-après :
• Single : traduire une seule adresse.
• Range : traduire une plage d'adresses.
• Subnet : traduire toutes les adresses dans le sous-réseau privé ou une partie du sous-réseau privé.</td></tr>
<tr><td>Range (plage)</td><td colspan="2">Saisissez le nombre d'adresses à traduire. Ce champ est disponible uniquement si vous choisissez Range (plage) dans le champ Type.
Valeurs valables : 1 à 128
Valeur par défaut = 1
IMPORTANT : chaque adresse dans la plage compte comme une entrée de traduction. Le switch prend en charge un maximum de 128 saisies de traduction.</td></tr>
<tr><td>Subnet Mask (masque de sous-réseau)</td><td colspan="2">Saisissez le masque de sous-réseau pour les adresses à traduire.
Valeurs valables :
• Classe B : 255.255.0.0
• Classe C : 255.255.255.0
• Portion de Classe C :
– 255 255 255 128 (fournit 128 adresses par entrée de traduction)
– 255 255 255 192 (fournit 64 adresses par entrée de traduction)
– 255 255 255 224 (fournit 32 adresses par entrée de traduction)
– 255.255.255.240 (fournit 16 adresses par entrée de traduction)</td></tr>
</table>

6. Cliquez sur l'onglet Public to Private.



7. Cliquez sur Add Row (ajouter une rangée), renseignez les champs, puis cliquez sur Save (enregistrer).

Champ	Description	
Public IP Address (adresse IP publique)	Saisissez une adresse IP publique : • Pour traduire une seule adresse, saisissez l'adresse existante pour le dispositif sur le sous-réseau public. • Pour traduire une plage d'adresses, saisissez la première adresse dans la plage d'adresses séquentielles. • Pour traduire des adresses dans un sous-réseau, saisissez l'adresse de départ actuelle de la plage de dispositifs sur le sous-réseau public. Cette adresse doit correspondre à la taille du masque de sous-réseau à traduire comme illustré ci-dessous.	
	Masque de sous-réseau	**Adresse de départ du sous-réseau public**
	255.255.0.0	Les deux derniers octets doivent se terminer par 0. **EXEMPLE :** 10.200.0.0
	255.255.255.0	Le dernier octet doit se terminer par 0. **EXEMPLE :** 10.200.1.0.
	255.255.255.128	Le dernier octet doit se terminer par 0 ou 128. **EXEMPLE :** 10.200.1.0 ou 10.200.1.128
	255.255.255.192	Le dernier octet doit correspondre à l'une des valeurs suivantes : 0, 64, 128, 192. **EXEMPLE :** 10.200.1.64
	255.255.255.224	Le dernier octet doit correspondre à l'une des valeurs suivantes : 0, 32, 64, 96, 128, 160, 192, 224. **EXEMPLE :** 10.200.1.32
	255.255.255.240	Le dernier octet doit correspondre à l'une des valeurs suivantes : 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240. **EXEMPLE :** 10.200.1.16

<table>
<tr><th>Champ</th><th>Description</th></tr>
<tr><td>Private IP Address (adresse IP privée)</td><td>Saisissez une adresse IP privée :
• Pour traduire une seule adresse, saisissez une adresse privée unique pour représenter le dispositif.
• Pour traduire une plage d'adresses, saisissez la première adresse dans la plage d'adresses séquentielles.
• Pour traduire des adresses dans un sous-réseau, saisissez une adresse privée de départ unique pour représenter les dispositifs. Cette adresse doit correspondre à la taille du masque de sous-réseau à traduire comme illustré ci-dessous.
<table>
<tr><th>Masque de sous-réseau</th><th>Adresse de départ du sous-réseau privé</th></tr>
<tr><td>255.255.0.0</td><td>Les deux derniers octets doivent se terminer par 0.
EXEMPLE : 192.168.0.0</td></tr>
<tr><td>255.255.255.0</td><td>Le dernier octet doit se terminer par 0.
EXEMPLE : 192.168.1.0</td></tr>
<tr><td>255.255.255.128</td><td>Le dernier octet doit se terminer par 0 ou 128.
EXEMPLE : 192.168.1.0 ou 192.168.1.128</td></tr>
<tr><td>255.255.255.192</td><td>Le dernier octet doit correspondre à l'une des valeurs suivantes : 0, 64, 128, 192.
EXEMPLE : 192.168.1.64</td></tr>
<tr><td>255.255.255.224</td><td>Le dernier octet doit correspondre à l'une des valeurs suivantes : 0, 32, 64, 96, 128, 160, 192, 224.
EXEMPLE : 192.168.1.32</td></tr>
<tr><td>255.255.255.240</td><td>Le dernier octet doit correspondre à l'une des valeurs suivantes : 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240.
EXEMPLE : 10.200.1.16</td></tr>
</table></td></tr>
<tr><td>Type</td><td>Choisissez l'une des valeurs ci-après :
• Single : traduire une seule adresse.
• Range : traduire une plage d'adresses.
• Subnet : traduire toutes les adresses dans le sous-réseau public ou une partie du sous-réseau public.</td></tr>
<tr><td>Range (plage)</td><td>Saisissez le nombre d'adresses à traduire. Ce champ est disponible uniquement si vous choisissez Range (plage) dans le champ Type.
Valeurs valables : 1 à 128
Valeur par défaut = 1
IMPORTANT : chaque adresse dans la plage compte comme une saisie de traduction. Le switch prend en charge un maximum de 128 saisies de traduction.</td></tr>
<tr><td>Subnet Mask (masque de sous-réseau)</td><td>Saisissez le masque de sous-réseau pour les adresses à traduire.
Valeurs valables :
• Classe B : 255.255.0.0
• Classe C : 255.255.255.0
• Portion de Classe C :
– 255 255 255 128 (fournit 128 adresses par entrée de traduction)
– 255 255 255 192 (fournit 64 adresses par entrée de traduction)
– 255 255 255 224 (fournit 32 adresses par entrée de traduction)
– 255.255.255.240 (fournit 16 adresses par entrée de traduction)</td></tr>
</table>

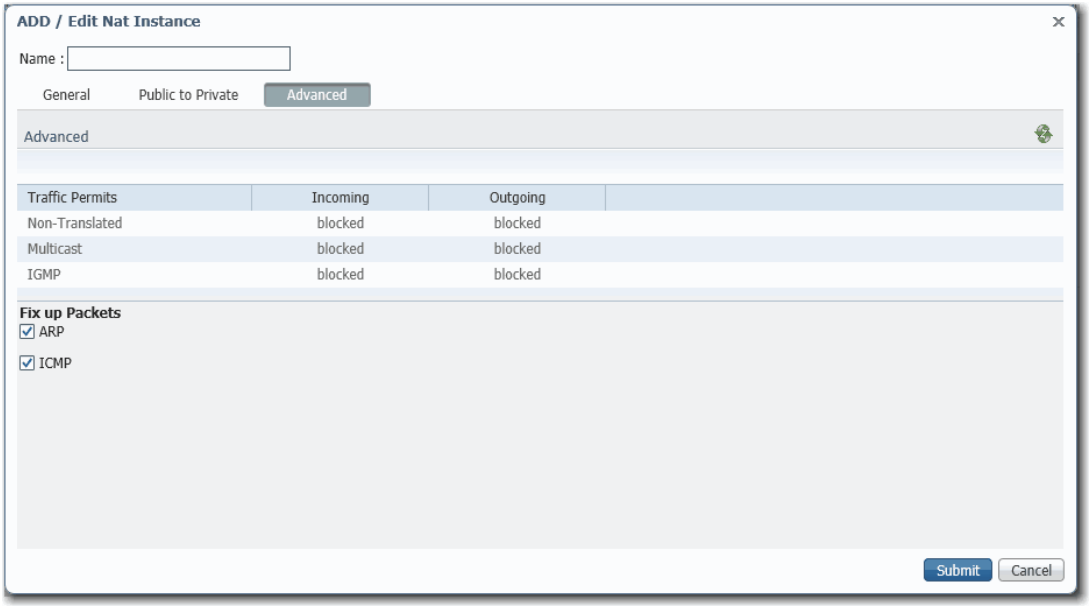
8. (facultatif). Pour configurer les autorisations de trafic et les corrections des paquets, poursuivez au paragraphe Configuration des permis et des corrections de trafic ci-dessous.
9. Sur la fenêtre NAT, cliquez sur Submit (soumettre).

Configuration des permis et des corrections de trafic

Soyez prudent lors de la configuration des permis et des corrections de trafic. Nous vous recommandons d'utiliser les valeurs par défaut.

Pour configurer les permis de trafic ou les corrections, suivez les étapes ci-après.

1. Cliquez sur l'onglet Advanced (avancé).



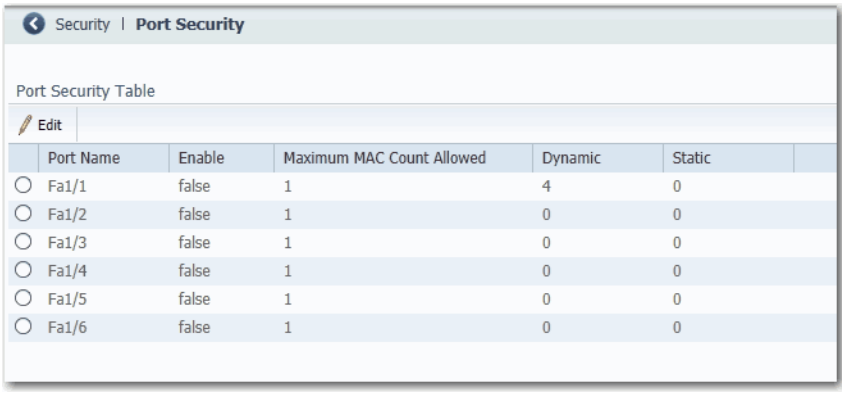
2. Choisissez l'une de ces options pour les paquets entrants et sortants qui ne sont pas manipulés par NAT :
   - Pass-through : autoriser les paquets à passer à travers la limite de NAT.
   - Blocked : les paquets sont abandonnés.
3. Dans la zone Fix up Packets (corriger les paquets), cochez ou décochez les cases pour activer ou désactiver les corrections pour ARP et ICMP.

   Par défaut, les corrections sont activées à la fois pour ARP et ICMP.
4. Cliquez sur Submit (soumettre).

Configuration de la sécurité de port

Configurer la sécurité du port afin de limiter les adresses MAC (MAC ID) qui peuvent avoir accès à un port donné. La sécurité du port est basée sur le nombre d'adresses MAC pris en charge (dont aucune n'est statiquement définie). La sécurité de port statique vous permet de spécifier si les adresses MAC sont apprises automatiquement ou définies manuellement.

Pour configurer la sécurité de port, dans le menu Configure, choisissez Port Security (sécurité de port).



La sécurité de port limite et identifie les adresses MAC des dispositifs qui peuvent envoyer du trafic à travers le port du switch. Le port du switch ne réachemine pas le trafic provenant des dispositifs à l'extérieur du groupe défini de dispositifs. Une violation de la sécurité se produit lorsqu'une des conditions suivantes se produit :

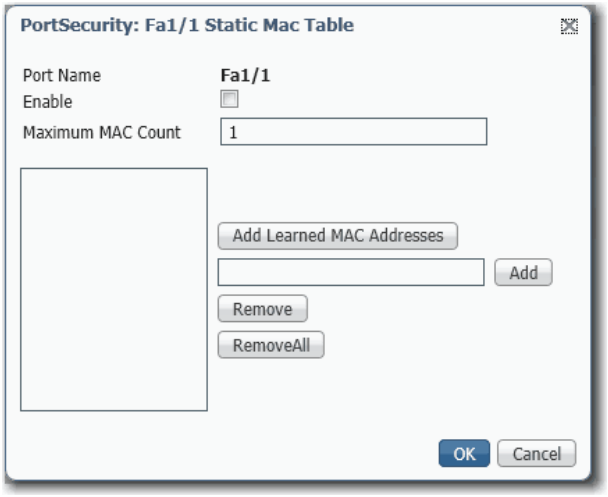
- Un dispositif, qui a une adresse MAC différente de toutes les adresses MAC sécurisées identifiées, tente d'accéder au port du switch.
- Le nombre d'adresses MAC sur le port dépasse le nombre maximum pris en charge sur le port.

La sécurité de port prend en charge les multiples niveaux de sécurité :

- La capacité de définir le nombre de dispositifs qui sont connectés à un port donné. Ceux-ci sont affectés sur une base de « premier venu, premier servi » et retirés après une certaine période d'inactivité.
- La capacité de facilement stocker la configuration d'une adresse MAC existante en sélectionnant Add Learned MAC Addresses (ajouter les adresses MAC apprises) dans la table Static MAC Address (adresse MAC statique).
- La capacité à ajouter et retirer des adresses MAC port par port.

Pour modifier la table Static MAC Addresses d'un port, effectuez les opérations suivantes :

1. Cliquez sur le bouton radio à côté du port à configurer.
2. Cliquez sur Edit (modifier).
3. Décochez ou cochez la case Enable (valider).
4. Configurez les adresses MAC comme suit :
   - Pour ajouter les adresses MAC existantes des dispositifs actuellement connectés à un port, cliquez sur Add Learned MAC Addresses (ajouter les adresses MAC apprises).
   - Pour ajouter une adresse MAC spécifique à la table, saisissez une adresse MAC dans les champs de format, puis cliquez sur Add (ajouter).
   - Pour retirer une adresse MAC de la table, sélectionnez l'adresse MAC, puis cliquez sur Remove (retirer).
   - Pour effacer la table d'adresses MAC, cliquez sur Remove All (tout retirer).



5. Cliquez sur OK.

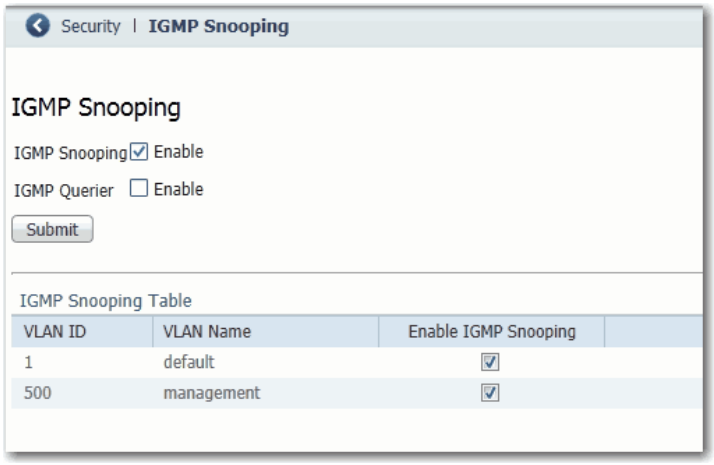
Configuration de la surveillance de trafic IGMP

La surveillance de trafic IGMP (Internet Group Management Protocol) réduit le trafic dupliqué et excédentaire sur le réseau en réacheminant le trafic IP en multidiffusion vers des ports de switch spécifiques plutôt que d'inonder tous les ports.

Avec la surveillance de trafic IGMP, seuls les ports qui sont membres de groupes IP spécifiques reçoivent les messages en multidiffusion. On obtient ainsi une utilisation plus efficace de la bande passante.

Pour configurer la surveillance de trafic, dans le menu Configure, choisissez IGMP Snooping (surveillance IGMP) :

- Pour activer la surveillance IGMP pour tous les VLAN ID, cochez Enable (valider) à côté de IGMP Snooping.
- Pour activer le demandeur IGMP pour tous les VLAN ID, cochez Enable (valider) à côté de IGMP Querier.
- Pour activer ou désactiver IGMP snooping sur un VLAN, sélectionnez le VLAN, puis cochez ou décochez la case Enable IGMP Snooping (valider la surveillance IGMP).

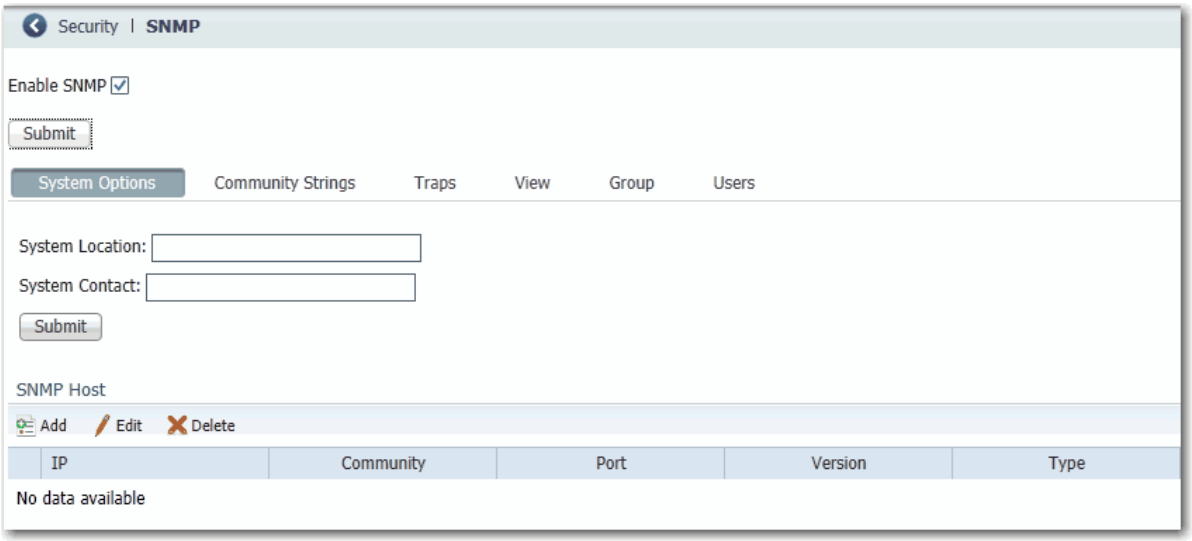


Configuration de SNMP

Activez SNMP si vous avez prévu de gérer le switch via une autre application de gestion de réseau. Par défaut, SNMP est désactivé.

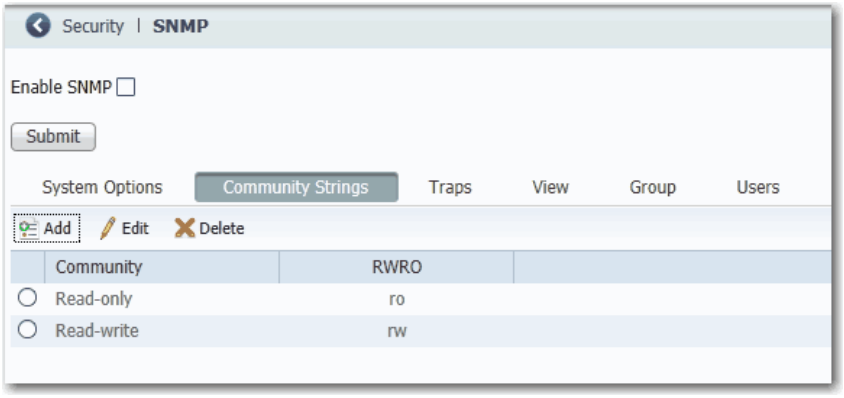
Parmi les autres réglages globaux de SNMP se trouvent le nom du switch ou de l'administrateur réseau et l'emplacement du switch. Le nom du système et les informations de contact du système s'affichent dans la zone Switch Information sur le tableau de bord.

Pour configurer SNMP, dans le menu Configure, choisissez SNMP.



Les chaînes de communauté sont des mots de passe pour accéder à la base MIB (Management Information Base) du switch. Vous pouvez créer des chaînes de communauté qui fournissent à un gestionnaire décentralisé un accès en lecture-seule ou en lecture-écriture au switch.

Pour créer, modifier et supprimer des chaînes de communauté, cliquez sur l'onglet Community Strings (chaînes de communauté).



Une chaîne de communauté en lecture seule permet au switch de valider les demandes Get (lecture-seule) provenant d'une station de gestion de réseau. Si vous définissez la communauté de lecture SNMP, les utilisateurs peuvent accéder aux objets de la MIB, mais ne peuvent pas les modifier.

Une chaîne de communauté en lecture-écriture permet au switch de valider les demandes Set (lecture-écriture) provenant d'une station de gestion de réseau.

Utilisation des applications de gestion de SNMP

Vous pouvez utiliser des applications de gestion de SNMP comme IntraVue ou HP OpenView pour configurer et gérer le switch. Reportez-vous à SNMP, à la page 90 pour plus d'informations.

Configuration des réglages d'alarme

Le logiciel du switch surveille en permanence les conditions des ports sur une base individuelle ou globale. Si les conditions ne correspondent pas aux paramètres définis, une alarme ou un message système est déclenché. Par défaut, le switch envoie les messages système à une installation de journalisation. Vous pouvez configurer le switch de façon à envoyer des pièges SNMP à un serveur SNMP. Vous pouvez également configurer le switch de façon à déclencher un dispositif d'alarme externe à l'aide des deux relais d'alarme indépendants.

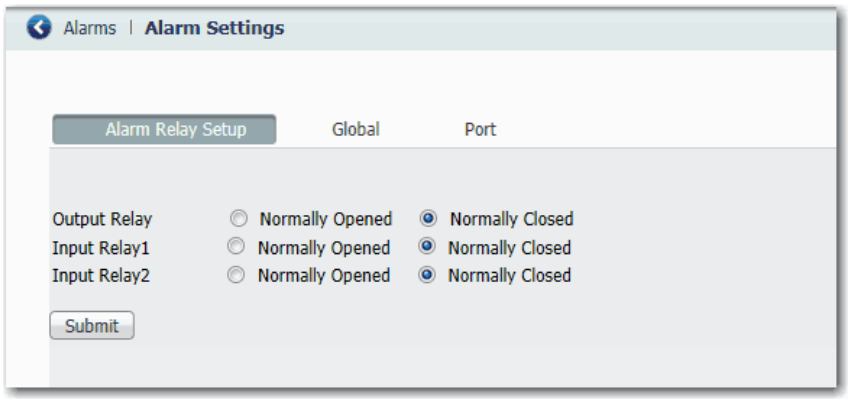
Réglages des relais d'alarme

Vous pouvez configurer le switch de façon à déclencher un dispositif d'alarme externe. Le switch prend en charge deux entrées d'alarme et une sortie d'alarme. Le logiciel du switch est configuré pour détecter les défauts qui sont utilisés pour mettre sous tension la bobine de relais et modifier l'état sur les deux contacts de relais. Les contacts normalement ouverts se ferment et les contacts normalement fermés s'ouvrent.

Pour configurer les réglages de relais d'alarme, dans le menu Configure, choisissez Alarm Settings (réglages d'alarme).

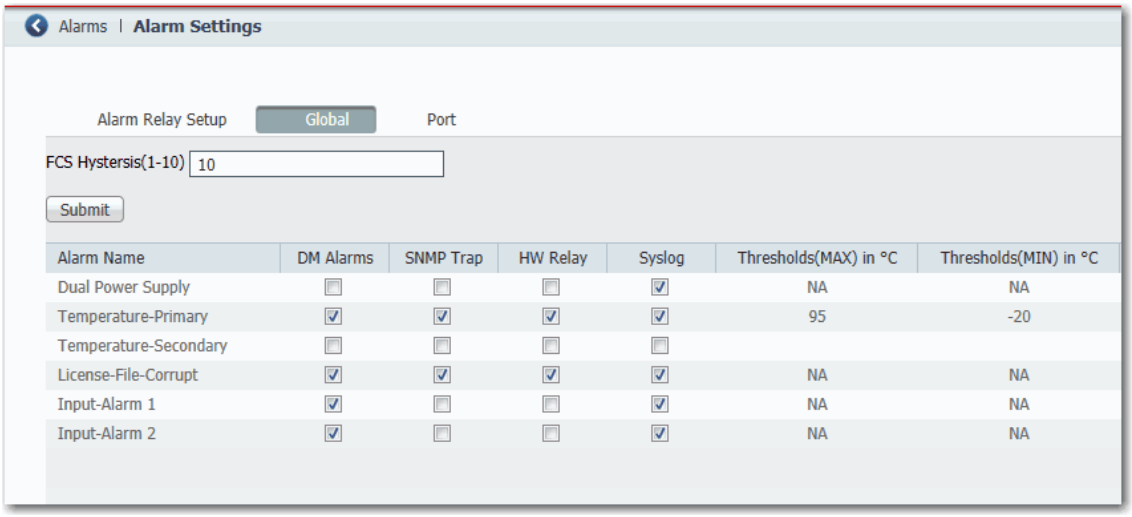
Dans l'onglet Alarm Relay Setup (configuration relais d'alarme), cliquez sur l'une de ces options pour chaque type de relais d'alarme :

- Normally Opened : la condition normale est qu'aucun courant ne circule à travers le contact. L'alarme est générée lorsque le courant passe.
- Normally Closed : la condition normale est que le courant circule à travers le contact. L'alarme est générée lorsque le courant cesse de circuler.



Alarmes globales

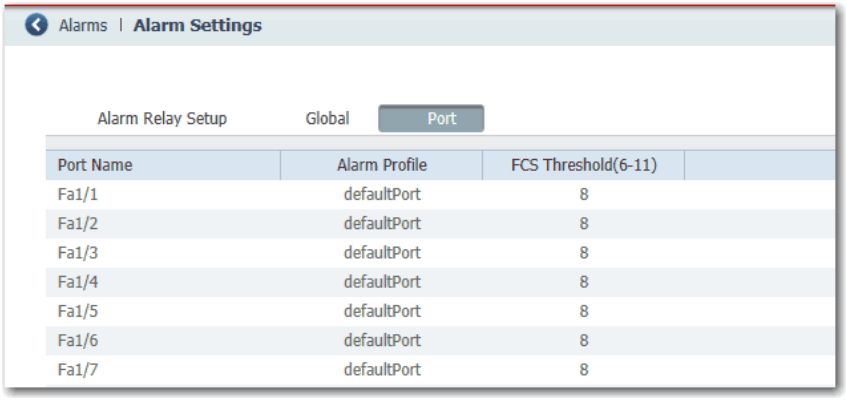
Pour configurer des alarmes globales, également connues sous le nom d'alarmes d'installation, dans le menu Configure, choisissez Alarm Settings (reglages d'alarme), puis cliquez sur l'onglet Global.



Champ	Description
FCS Hysteresis (1-10)	Le seuil d'hystérésis d'erreur de la séquence de contrôle de trame (FCS) est utilisé pour déterminer quand une condition d'alarme est désactivée. Cette valeur est exprimée en pourcentage de la fluctuation du taux d'erreur de bit FCS. Le réglage par défaut est 8 pour cent. Vous pouvez ajuster le pourcentage pour empêcher le basculement de l'état d'alarme lorsque le taux d'erreur de bit FCS fluctue près du taux d'erreur de bit configuré. Les pourcentages valables pour les réglages globaux sont entre 1 et 10. Ce réglage peut également être configuré sur un port individuel via l'onglet Port.
Alarm Name (nom d'alarme)	Les types d'alarmes pouvant être activés ou désactivés sont : • Dual Power Supply : le switch surveille les niveaux d'alimentation c.c. Si le système est configuré pour fonctionner en mode de double alimentation, une alarme est déclenchée si une alimentation défaille ou manque. L'alarme est automatiquement désactivée lorsque les sources d'alimentation sont présentes ou fonctionnent. Vous pouvez configurer l'alarme d'alimentation de façon à la connecter aux relais matériels. • Temperature-Primary : ces alarmes sont déclenchées lorsque la température du système est plus élevée ou plus basse que les seuils configurés. Par défaut, l'alarme de température principale est associée au relais principal. • Temperature-Secondary : ces alarmes sont déclenchées lorsque la température du système est plus élevée ou plus basse que les seuils configurés. • License-File-Corrupt : une alarme est déclenchée lorsque le fichier de licence est endommagé. • Input-Alarm 1 : une alarme est déclenchée en fonction d'une entrée d'alarme externe. • Input-Alarm 2 : une alarme est déclenchée en fonction d'une entrée d'alarme externe.
DM Alarms (alarmes DM)	Les informations de l'alarme s'affichent sur le tableau de bord de l'interface Internet de Device Manager.
SNMP Trap (piège SNMP)	Les pièges d'alarme seront envoyés à un serveur SNMP, si SNMP est activé dans la fenêtre Configure > Security > SNMP.
HW Relay (relais matériel)	Le relais d'alarme du switch est déclenché et envoie un signal de défaut à un dispositif d'alarme externe connecté, tel qu'une sonnerie, une lumière ou un autre dispositif de signalisation que vous avez configuré.
Syslog	Les pièges d'alarme sont enregistrés dans le syslog. Vous pouvez afficher le syslog dans la fenêtre Monitor > Syslog (Affichage Syslog).
Thresholds (MAX) (seuils maxi.) en °C	Le seuil de température maximum pour l'alarme Temperature-Primary ou Temperature-Secondary correspondante, le cas échéant.
Thresholds (MIN) (seuils mini.) en °C	Le seuil de température minimum pour l'alarme Temperature-Primary ou Temperature-Secondary correspondante, le cas échéant.

Alarmes de port

Pour créer des profils d'alarme pour les ports individuels, dans le menu Configure, choisissez Alarm Settings (reglages d'alarme), puis cliquez sur l'onglet Port.



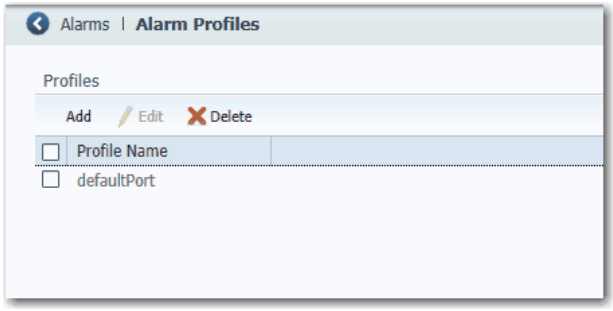
Pour chaque port, choisissez un Alarm Profile (profil d'alarme) et définissez le seuil FCS. Le seuil d'hystérésis d'erreur de la séquence de contrôle de trame (FCS) est exprimé en pourcentage de la fluctuation du taux d'erreur de bit FCS. Le réglage par défaut est 8 pour cent. Vous pouvez ajuster le pourcentage pour empêcher le basculement de l'état d'alarme lorsque le taux d'erreur de bit FCS fluctue près du taux d'erreur de bit configuré. Les pourcentages valides pour les réglages de port sont entre 6 et 11.

Configuration des paramètres d'alarme

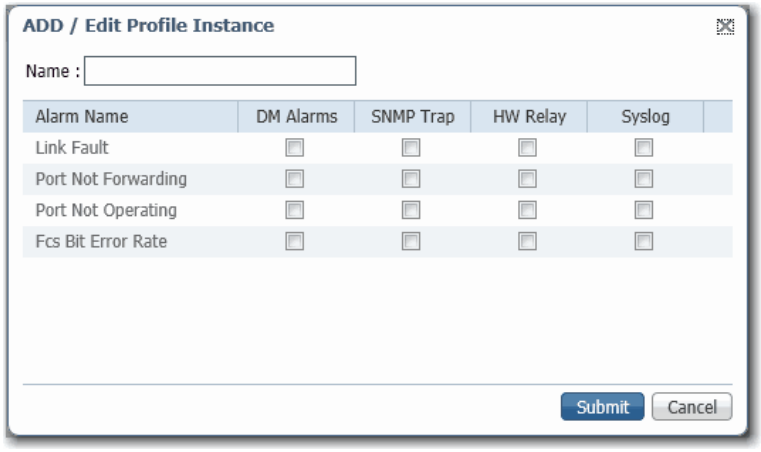
Vous pouvez utiliser des profils d'alarme pour appliquer un groupe de réglages d'alarme à plusieurs interfaces. Ces profils d'alarme sont créés pour vous :

- defaultPort
- ab-alarm (créé pendant Express Setup)

Pour créer, modifier ou supprimer des profils d'alarme, dans le menu Configure, choisissez Alarm Profiles (profils d'alarme).



Dans la fenêtre Add/Edit Profile Instance (ajouter/modifier une instance de profil), vous pouvez configurer les alarmes et les actions pour le profil d'alarme.



Champ	Description
Name (nom)	Un nom unique pour le profil d'alarme.
Alarm Name (nom d'alarme)	Ces types d'alarmes peuvent déclencher une action.
DM Alarms (alarmes DM)	Les informations de l'alarme s'affichent sur le tableau de bord de l'interface Internet de Device Manager.
SNMP Trap (piège SNMP)	Les pièges d'alarme seront envoyés à un serveur SNMP, si SNMP est activé dans la fenêtre Configure > Security > SNMP.
HW Relay (relais matériel)	Le relais d'alarme du switch est déclenché et envoie un signal de défaut à un dispositif d'alarme externe connecté, tel qu'une sonnerie, une lumière ou un autre dispositif de signalisation que vous avez configuré.
Syslog	Les pièges d'alarme sont enregistrés dans le syslog. Vous pouvez afficher le syslog dans la fenêtre Monitor > Syslog (Affichage Syslog).

Surveillance des tendances

Vous pouvez afficher des données historiques pour vous aider à analyser les modèles de trafic et identifier les problèmes. Les données peuvent être affichées en incréments de secondes, minutes, heures ou jours.

Pour afficher les données dans une table, cliquez sur le bouton Grid Mode en dessous de la zone. Pour afficher un graphique, cliquez sur le bouton Chart Mode. Utilisez les liens 60 s, 1 h, 1 d et 1 w pour afficher les données par incréments de 60 secondes, 1 heure, 1 jour ou 1 semaine.

Afin de surveiller les tendances, dans le menu Monitor (affichage), choisissez Trends tendances).

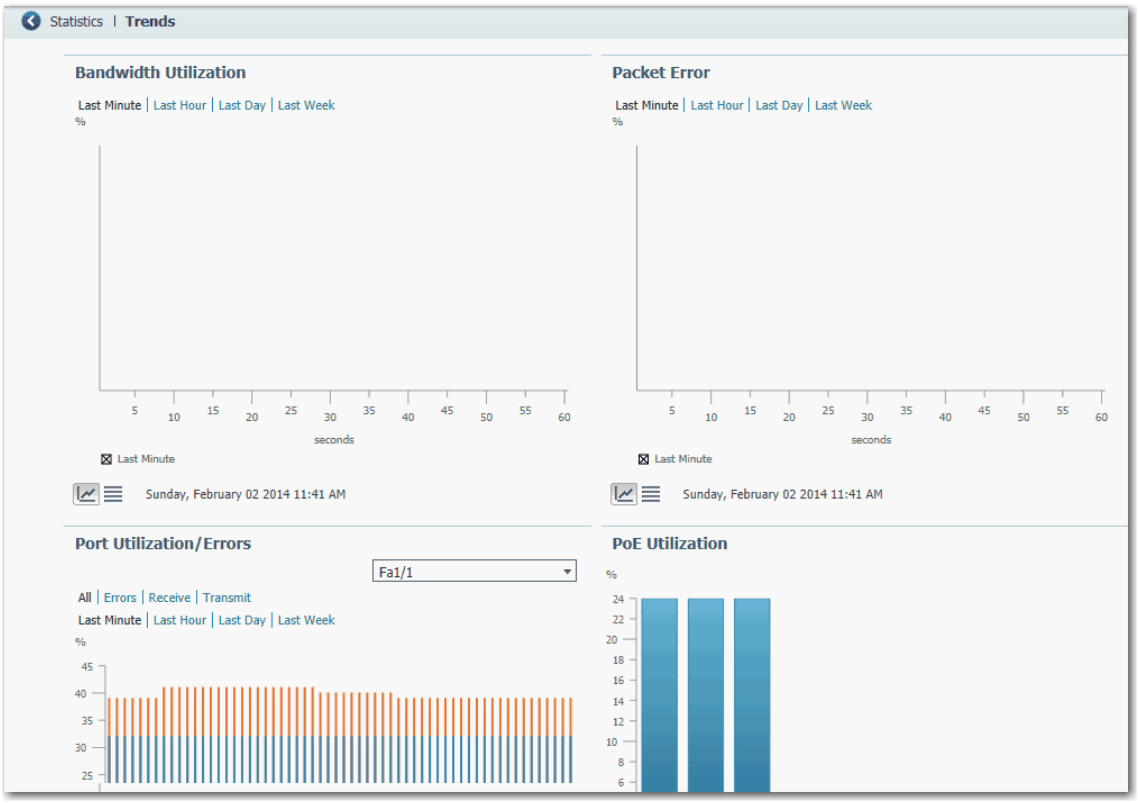


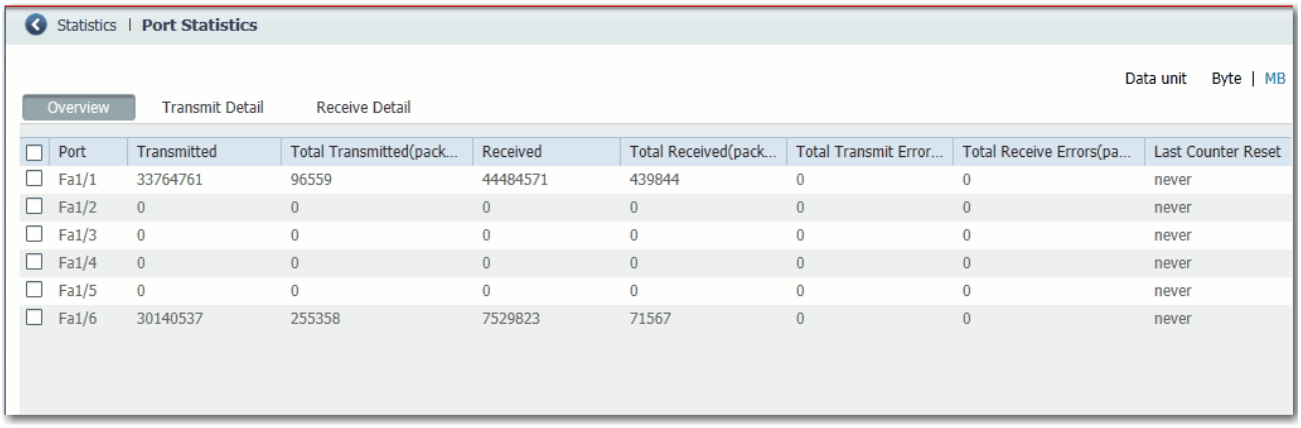
Tableau 17 - Graphiques de tendances

Graphique	Description
Bandwidth Utilization (utilisation de la bande passante)	Le graphique Bandwidth Utilization indique le pourcentage de la bande passante disponible qui a été utilisé. Le graphique peut montrer l'utilisation de la bande passante au cours d'instances incrémentielles exprimées en temps (par 60 secondes, 60 minutes, 24 heures ou 14 jours). Ce graphique marque également le pic le plus élevé atteint. La valeur par défaut est 60 secondes. Vous pouvez utiliser ces données pour déterminer le taux d'utilisation du réseau.
Packet Error (erreur de trame)	Le graphique Packet Error montre le pourcentage d'erreurs de trame collecté au cours d'instances incrémentielles exprimées en temps (par 60 secondes, 60 minutes, 24 heures, ou 14 jours). La valeur par défaut est 60 secondes. Utilisez ce graphique pour contrôler les effets que les dispositifs connectés ont sur les performances du switch ou du réseau. Par exemple, si vous soupçonnez qu'un dispositif connecté envoie des paquets d'erreurs, vous pouvez vérifier si les données sur le graphique changent lorsque vous déconnectez et reconnectez le dispositif suspect.
Port Utilization/Errors (utilisation/erreurs de port)	Le graphique Port Utilization/Errors montre les modèles d'utilisation d'un port spécifique au cours d'instances incrémentielles exprimées en temps (par 60 secondes, 60 minutes, 24 heures ou 14 jours). La valeur par défaut est 60 secondes. Pour afficher les tendances pour un port spécifique, choisissez un port de la liste Port. Utilisez ces graphiques pour observer les performances d'un port spécifique. Par exemple, si un utilisateur de réseau a une connectivité réseau intermittente, utilisez le graphique Port Utilization afin d'observer les modèles de trafic sur le port auquel l'ordinateur personnel de l'utilisateur est connecté et utilisez le graphique Port Errors pour voir si le port reçoit ou envoie des paquets d'erreurs.
PoE Utilization (utilisation de PoE)	Pour les switchs PoE, le graphique PoE Utilization montre la puissance qui est allouée aux dispositifs connectés.

Surveillance des statistiques de port

Vous pouvez afficher les statistiques pour les données envoyées et reçues par les ports de switch depuis sa dernière mise sous tension ou depuis le dernier effacement des statistiques.

Pour surveiller les statistiques de port, dans le menu Monitor (surveillance), choisissez Port Statistics (statistiques de port). Pour plus d'informations, consultez l'aide en ligne de l'interface Internet de Device Manager.



Port	Transmitted	Total Transmitted(pack...	Received	Total Received(pack...	Total Transmit Error...	Total Receive Errors(pa...	Last Counter Reset
Fa1/1	33764761	96559	44484571	439844	0	0	never
Fa1/2	0	0	0	0	0	0	never
Fa1/3	0	0	0	0	0	0	never
Fa1/4	0	0	0	0	0	0	never
Fa1/5	0	0	0	0	0	0	never
Fa1/6	30140537	255358	7529823	71567	0	0	never

Les types de statistiques de port recueillies et affichées sont regroupés sous ces onglets dans la fenêtre Port Statistics de l'interface Internet de Device Manager :

- Onglet Overview : utilisez cet onglet pour afficher les nombres spécifiques de paquets d'erreurs reçus sur et envoyés depuis le port (ce niveau de détail n'est pas disponible depuis les graphiques du tableau de bord).

  Le nombre de paquets d'erreurs peut signifier une discordance de duplex, des incompatibilités avec le port et le dispositif connecté ou des câbles ou dispositifs défectueux. Ces problèmes peuvent tous provoquer un ralentissement des performances réseau, une perte de données ou un manque de connectivité.

- Onglet Transmit Detail : utilisez cet onglet pour résoudre les problèmes des changements inhabituels dans le trafic réseau. Cet onglet affiche les statistiques suivantes :

  – Les paquets en envoi individuel, multidiffusion ou diffusion générale envoyés de chaque port
  – Des statistiques détaillées concernant les erreurs envoyées à chaque port

  Si un port envoie une quantité anormalement élevée de trafic (tels que des paquets en multidiffusion ou en diffusion générale), surveillez le dispositif connecté pour voir si ce modèle de trafic est normal ou s'il peut signifier un problème.

- Onglet Receive Detail : utilisez cet onglet pour résoudre les problèmes de modification anormale du trafic sur le réseau. Cet onglet affiche les statistiques suivantes :

  – Les paquets en envoi individuel, multidiffusion ou diffusion générale reçus sur chaque port
  – Des statistiques détaillées des erreurs reçues sur chaque port

  Si un port reçoit une quantité anormalement élevée de trafic (tels que des paquets en multidiffusion ou en diffusion générale), surveillez le dispositif connecté pour voir si ce modèle de trafic est normal ou s'il peut signifier un Surveillance des statistiques NAT.

Surveillance des statistiques NAT

Vous pouvez surveiller les types de statistiques NAT suivants :

- Statistiques globales pour toutes les instances
- Statistiques par instance
- Traductions privées détaillées par instance
- Traductions publiques détaillées par instance

Pour afficher la fenêtre NAT Statistics, dans le menu Monitor (surveillance), choisissez NAT Statistics (statistiques NAT).

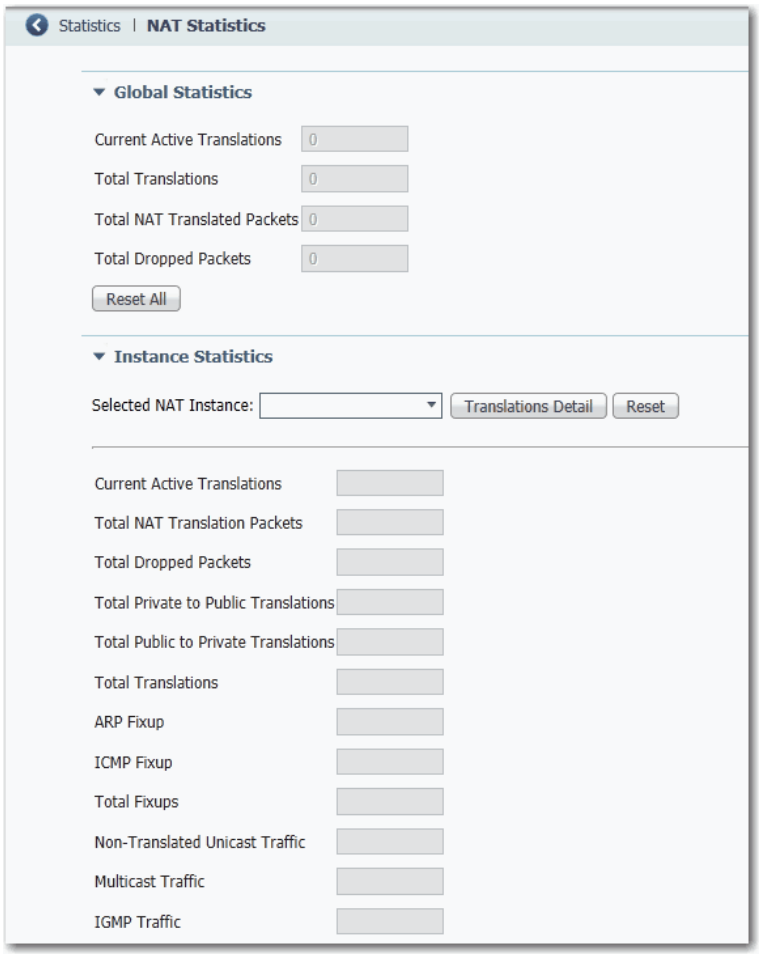


Tableau 18 - Statistiques globales NAT

Champ	Description
Current Active Translations (traductions actives actuelles)	Le nombre d'adresses IP qui ont été traduites au cours des dernières 90 secondes dans toutes les instances NAT.
Total Translations (traductions totales)	Le nombre total de traductions dans toutes les instances NAT.
Total NAT Translated Packets (paquets NAT traduits totaux)	Le nombre total de paquets dans toutes les instances NAT.
Total Dropped Packets (paquets rejetés totaux)	Le nombre total de paquets qui ont été rejetés dans toutes les instances NAT.

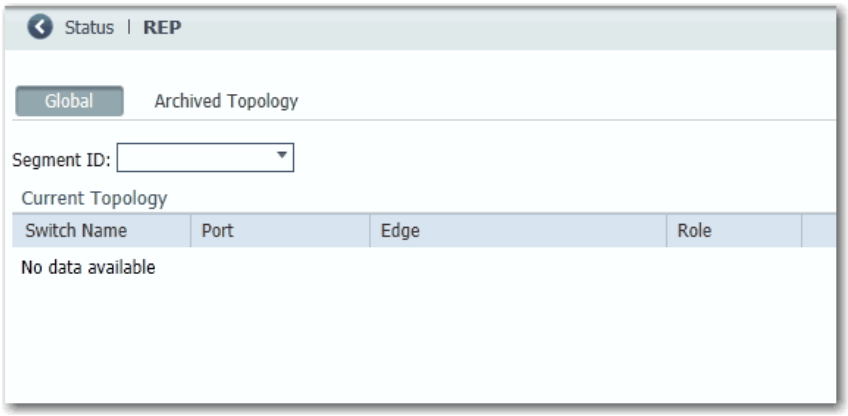
Tableau 19 - Statistiques de l'instance

Champ	Description
Selected Instance (instance sélectionnée)	Dans le menu déroulant, choisissez l'instance dont vous voulez afficher les statistiques.
Current Active Translations (traductions actives actuelles)	Le nombre de traductions qui ont eu lieu au cours des dernières 90 secondes pour l'instance.
Total NAT Translated Packets (paquets NAT traduits totaux)	Le nombre total de paquets qui ont été traduits pour l'instance.
Total Dropped Packets (paquets rejetés totaux)	Le nombre total de paquets qui ont été rejetés pour l'instance.
Total Private to Public Address Translations (traductions d'adresse privée à publique totales)	Le nombre total de traductions configurées pour les dispositifs sur le sous-réseau privé.
Total Private to Public Address Translations (traductions d'adresse publique à privée totales)	Le nombre total de traductions configurées pour les dispositifs sur le sous-réseau privé.
Total Translations (traductions totales)	Le nombre total de traductions configurées pour l'instance.
ARP Fixup (correction ARP)	Le nombre de paquets ARP qui ont été corrigés pour l'instance.
ICMP Fixup (correction ICMP)	Le nombre de paquets ICMP qui ont été corrigés pour l'instance.
Total Fixups (corrections totales)	Le nombre total de paquets ARP et ICMP qui ont été corrigés pour l'instance.
Non-Translated Unicast Traffic (trafic d'envoi individuel non traduit)	Le nombre de paquets avec du trafic en envoi individuel non traduit pour l'instance.
Multicast Traffic (trafic multidiffusion)	Le nombre de paquets avec du trafic en multidiffusion pour l'instance.
IGMP Traffic (trafic IGMP)	Le nombre de paquets avec du trafic IGMP pour l'instance.

Surveillance de la topologie REP

Pour examiner la topologie REP pour l'un des segments du réseau ou l'ensemble des segments, dans le menu Monitor (surveillance) , choisissez REP.

Pour afficher une topologie REP archivée, cliquez sur l'onglet Archived Topology (topologie archivée), puis sélectionnez l'ID du segment.



Surveillance de l'état CIP

CIP (Common Industrial Protocol) est un protocole de messagerie de couche d'application utilisé par divers dispositifs d'automatisation industrielle et de commande pour communiquer au sein d'un système de commande. CIP est la couche d'application pour le réseau EtherNet/IP. Les switchs Stratix contiennent un serveur EtherNet/IP qui permet au switch de faire partie du système d'automatisation et de commande industriel pour la surveillance et la gestion de base.

La fenêtre CIP Status affiche des informations sur l'état (champ Overview) et les statistiques (champ Request Details) du CIP depuis la dernière fois que le switch a été mis sous tension, redémarré ou les compteurs réinitialisés.

Pour résoudre un problème, réinitialisez les compteurs de CIP et voyez si les compteurs montrent que le problème existe encore.

IMPORTANT À l'exception d'Active Multicast Groups, toutes les catégories sont liées au serveur CIP sur le switch ; elles sont donc liées au trafic CIP spécialement dirigé vers le switch comme dispositif cible CIP. Elles ne renvoient pas au trafic CIP (EtherNet/IP) qui circule via le switch entre les divers automates CIP, les dispositifs IHM, les outils de configuration ou d'autres dispositifs cibles CIP, tels que des variateurs, des modules d'E/S, des démarreurs de moteur, des capteurs et des vannes.

Pour surveiller l'état du CIP, dans le menu Monitor (surveillance), choisir CIP Status (état CIP).

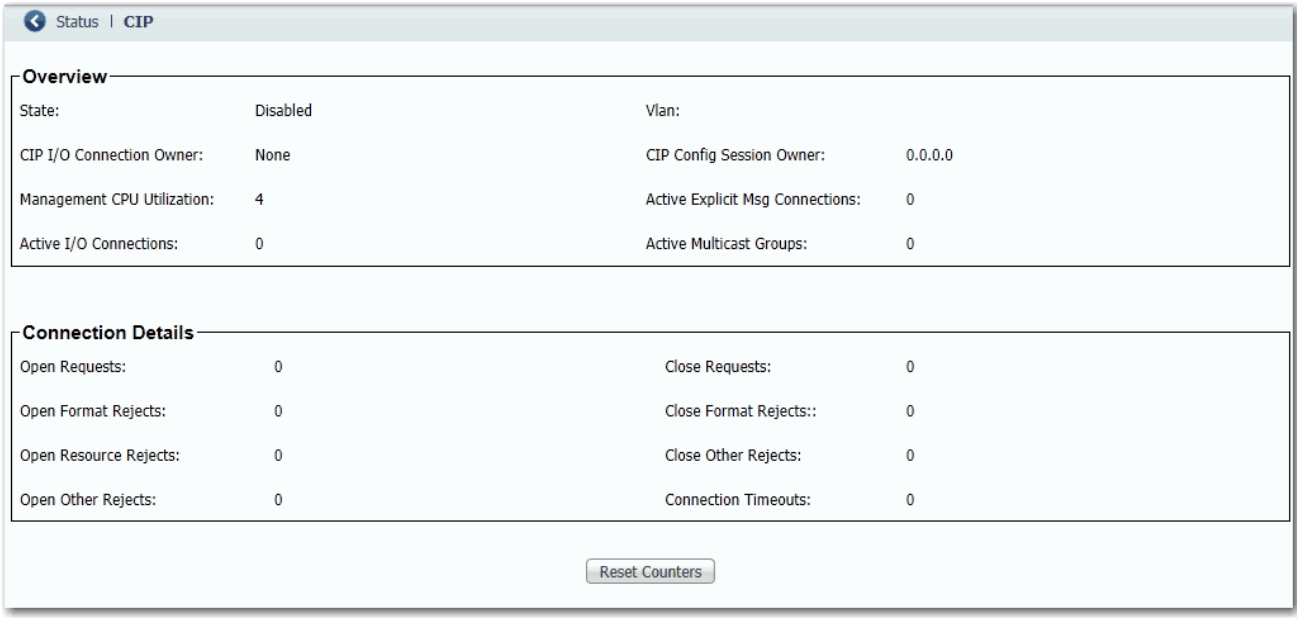


Tableau 20 - Champs d'état CIP

Champ	Description
Présentation	
State (état)	L'état de la connexion CIP (Enabled ou Disabled) (activé ou désactivé).
Vlan	L'ID du VLAN.
CIP I/O Connection Owner (propriétaire de la connexion d'E/S CIP)	L'adresse IP du switch vers et depuis laquelle des données de sortie d'E/S spécifiques aux applications sont envoyées et reçues.
CIP Config Session Owner (propriétaire de la session config. CIP)	L'adresse IP du dispositif contrôlant la session de configuration de CIP.
Management CPU Utilization (%) (utilisation de la CPU de gestion)	Le pourcentage de l'unité centrale de gestion utilisé pour les fonctions de gestion. Les fonctions du switch ont des ASICs dédiés qui ne sont pas impactés par les fonctions de gestion.
Active Explicit Msg Connections (connexions de Msg explicite actives)	Le nombre de connexions de messagerie explicite actives avec le switch comme cible.
Active I/O Connections (connexions d'E/S actives)	Le nombre de connexions d'E/S actives avec le switch comme cible.
Active Multicast Groups (groupes de multidiffusion actifs)	Le nombre de groupes de multidiffusion, y compris les groupes de multidiffusion CIP, circulant à travers le switch.
Détails de connexion	
Open Requests (requêtes ouvertes)	Le nombre de requêtes Forward Open reçues par le switch pour établir une connexion avec le switch.
Close Requests (requêtes fermées)	Le nombre de requêtes Forward Close reçues par le switch après qu'une connexion réussie a été établie avec le switch.
Open Format Rejects (rejets de format d'ouverture)	Le nombre de requêtes Forward Open dirigées vers le switch qui ont échoué, car la requête n'avait pas un format valide.
Close Format Rejects (rejets de format de fermeture)	Le nombre de requêtes Forward Close dirigées vers le switch qui ont échoué, car la requête n'avait pas un format valide.
Open Resource Rejects (rejets d'ouverture de ressource)	Le nombre de requêtes Forward Open qui n'ont pas réussi à établir une nouvelle connexion pour des raisons telles qu'une mémoire insuffisante.
Close Other Rejects (autres rejets de fermeture)	Le nombre de requêtes Forward Close qui ont échoué pour des raisons telles qu'un détrompage électronique incompatible.
Open Other Rejects (autres rejets d'ouverture)	Le nombre de requêtes Forward Open qui ont échoué pour des raisons telles qu'un détrompage électronique incompatible.
Connection Timeouts (timeouts de connexion)	Le nombre de connexions CIP qui ont expiré pour cause d'inactivité.

Diagnostic des problèmes de câblage

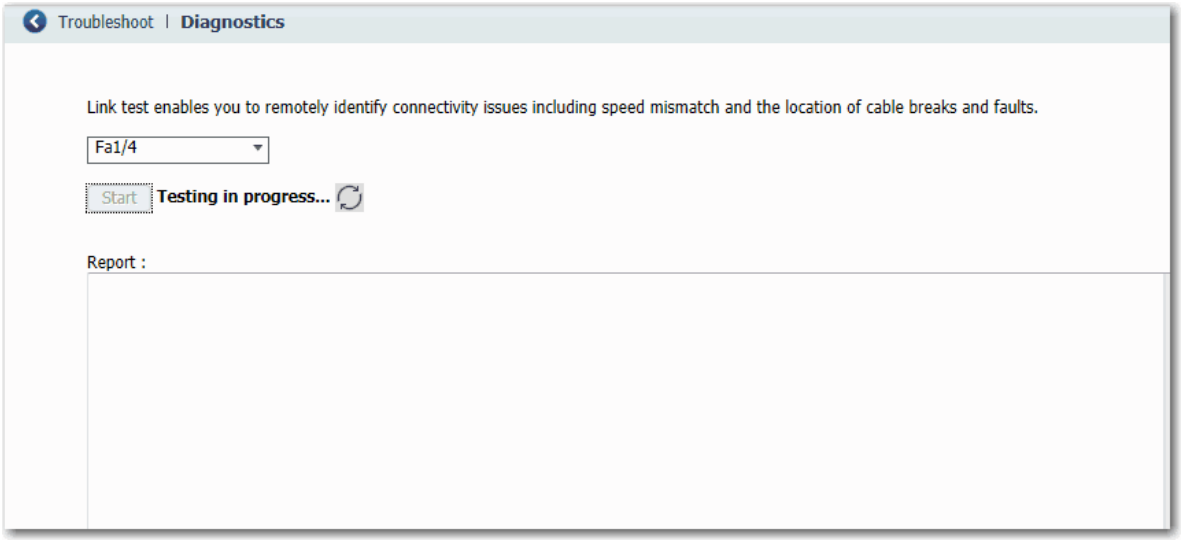
Utilisez la fenêtre Diagnostics pour exécuter le test de détection de fil coupé (Broken Wire Detection) qui utilise la détection de la réflectométrie de domaine temporel (TDR) pour identifier, diagnostiquer et résoudre les problèmes de câblage. La détection de TDR est prise en charge sur les ports cuivre Ethernet 10/100 et 10/100/1 000. La TDR n'est pas prise en charge sur les ports de module enfichable à faible encombrement (SFP).

Le test de liaison peut interrompre le trafic entre le port et le dispositif connecté. Ne lancez ce test que si vous suspectez un problème sur un port. Avant de lancer le test de liaison, utilisez la vue Front Panel, les fenêtres Port Status et Port Statistics pour recueillir des informations sur un problème potentiel.

IMPORTANT Pour lancer un test valide sur des ports gigabit, vous devez d'abord configurer le port gigabit comme un type de support RJ45, tel que décrit dans la section Configuration des paramètres de port à la page 109.

Pour diagnostiquer un câblage, dans le menu Monitor (surveillance), choisissez Diagnostics.

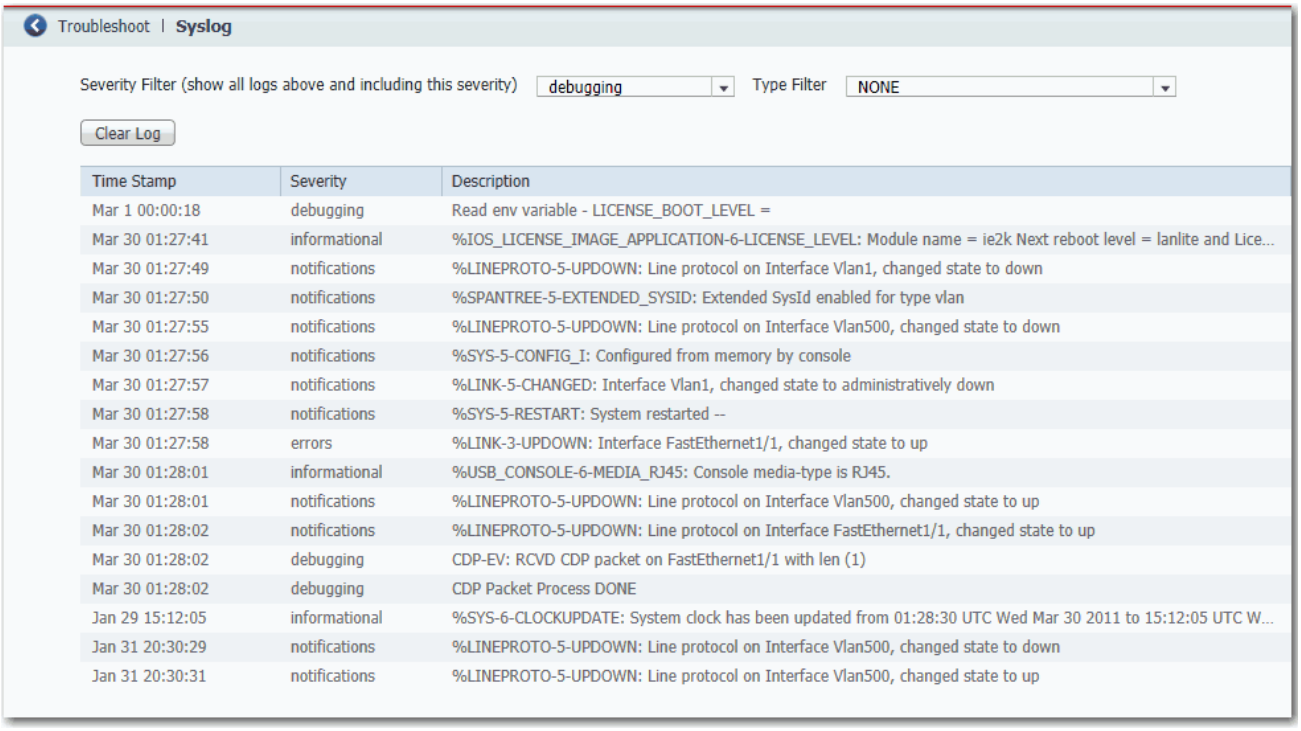
Pour lancer un test, sélectionnez un port, puis cliquez sur Start (démarrer).



Affichage des messages du journal système

Le journal système affiche des événements survenus sur le dispositif et ses ports, selon les réglages d'alarme que vous configurez dans la fenêtre Configure > Alarm Settings (configuration des réglages d'alarme).

Pour voir les messages du journal système, dans le menu Monitor (surveillance), choisissez Syslog.



Time Stamp	Severity	Description
Mar 1 00:00:18	debugging	Read env variable - LICENSE_BOOT_LEVEL =
Mar 30 01:27:41	informational	%IOS_LICENSE_IMAGE_APPLICATION-6-LICENSE_LEVEL: Module name = ie2k Next reboot level = lanlite and Lice...
Mar 30 01:27:49	notifications	%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
Mar 30 01:27:50	notifications	%SPANTREE-5-EXTENDED_SYSID: Extended SysId enabled for type vlan
Mar 30 01:27:55	notifications	%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan500, changed state to down
Mar 30 01:27:56	notifications	%SYS-5-CONFIG_I: Configured from memory by console
Mar 30 01:27:57	notifications	%LINK-5-CHANGED: Interface Vlan1, changed state to administratively down
Mar 30 01:27:58	notifications	%SYS-5-RESTART: System restarted --
Mar 30 01:27:58	errors	%LINK-3-UPDOWN: Interface FastEthernet1/1, changed state to up
Mar 30 01:28:01	informational	%USB_CONSOLE-6-MEDIA_RJ45: Console media-type is RJ45.
Mar 30 01:28:01	notifications	%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan500, changed state to up
Mar 30 01:28:02	notifications	%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/1, changed state to up
Mar 30 01:28:02	debugging	CDP-EV: RCVD CDP packet on FastEthernet1/1 with len (1)
Mar 30 01:28:02	debugging	CDP Packet Process DONE
Jan 29 15:12:05	informational	%SYS-6-CLOCKUPDATE: System clock has been updated from 01:28:30 UTC Wed Mar 30 2011 to 15:12:05 UTC W...
Jan 31 20:30:29	notifications	%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan500, changed state to down
Jan 31 20:30:31	notifications	%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan500, changed state to up

Pour filtrer des événements historiques, choisissez un filtre de sévérité ou un filtre de type :

- Debugging : messages de débogage.
- Informational : messages d'information.
- Notifications : le switch fonctionne normalement, mais présente une condition notable.
- Warnings : le switch présente une condition d'avertissement.
- Errors : le switch présente une condition d'erreur.
- Critical : le switch présente une condition critique.
- Alerts : le switch requiert une action immédiate.
- Emergencies : le switch est inutilisable.

Cliquez sur Clear Log (effacer le journal)pour indiquer que vous avez lu les alertes. Le fait de cliquer sur Clear Log ne résout pas le problème.

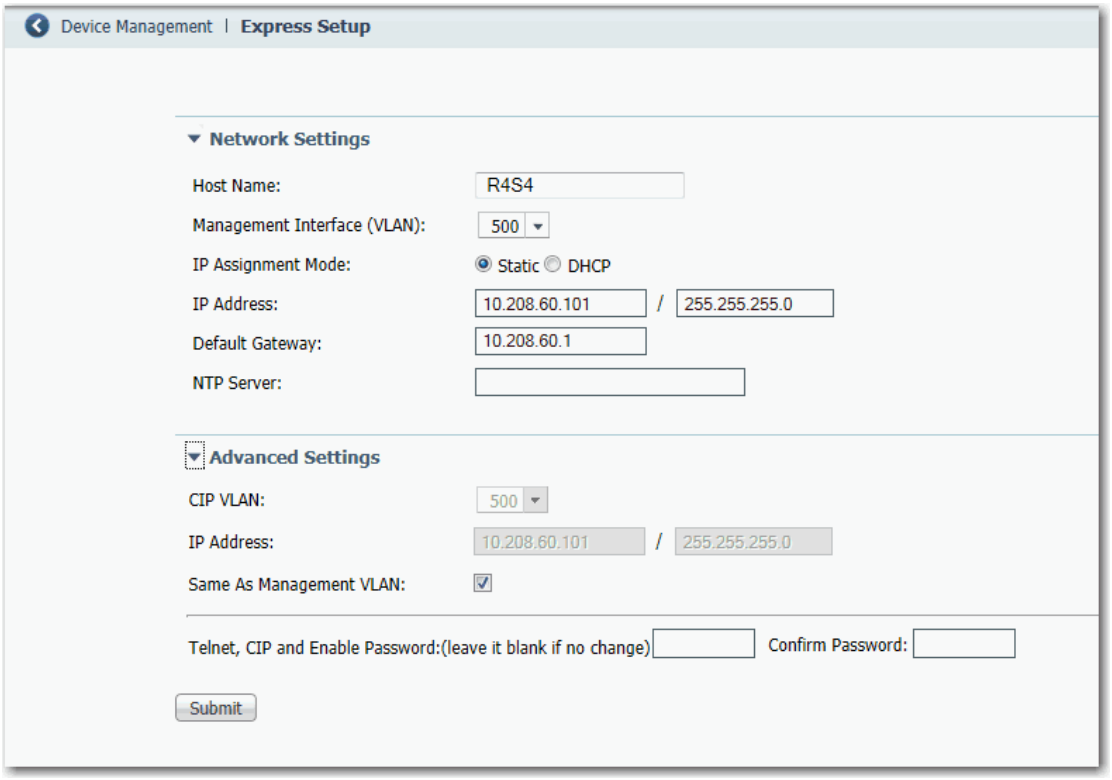
Tableau 21 - Champs de syslog

Champ	Description
Time Stamp (horodatage)	La date et l'heure auxquelles l'événement a eu lieu. Utilisez la fenêtre Express Setup pour relier le dispositif à un serveur NTP. Les paramètres de temps sont perdus si le switch n'est plus alimenté.
Severity Level (niveau de gravité)	Le type et la gravité de l'événement.
Description	La description du problème, y compris le port sur lequel le problème a été détecté.

Utilisation d'Express Setup pour changer les réglages du switch

Les réglages de réseau activent le switch de façon à fonctionner avec les réglages par défaut standard ; il sera géré via l'interface Internet de Device Manager. Ces réglages ont été définis lors de la configuration initiale. Modifiez ces réglages si vous souhaitez déplacer le switch vers un autre VLAN de gestion ou un autre réseau.

Pour mettre à jour les informations IP du switch, dans le menu Admin, choisissez Express Setup.

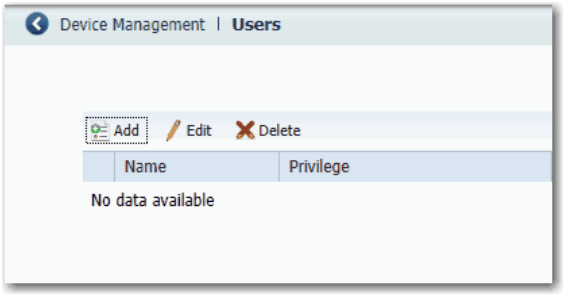


Champ	Description
	Réglages réseau
Host Name (nom d'hôte)	Le nom du dispositif.
Management Interface (interface de gestion – VLAN ID)	Le nom et l'ID du VLAN de gestion à travers lequel le switch est géré. Choisissez un VLAN existant qui sera le VLAN de gestion. L'ID par défaut est 1. Le nom par défaut pour le VLAN de gestion est « default ». Le nombre peut être entre 1 et 1 001. Assurez-vous que le switch et la station de gestion de votre réseau sont dans le même VLAN. Dans le cas contraire, vous perdez la connectivité de gestion du switch. Le VLAN de gestion est le domaine de diffusion générale à travers lequel le trafic de gestion est envoyé entre des utilisateurs ou dispositifs spécifiques. Il fournit le contrôle de diffusion générale et la sécurité pour le trafic de gestion qui doivent être limités à un groupe spécifique d'utilisateurs, tels que les administrateurs de votre réseau. Il fournit également un accès administratif sécurisé à tous les dispositifs du réseau, et ce, en permanence.
IP Assignment Mode (mode attribution IP)	Le mode d'attribution IP détermine si les informations IP du switch sont affectées manuellement (statiques) ou affectées automatiquement par un serveur DHCP (Dynamic Host Configuration Protocol). La valeur par défaut est Static. Nous vous recommandons d'utiliser Static et d'attribuer manuellement l'adresse IP du switch. Vous pouvez ensuite utiliser la même adresse IP chaque fois que vous souhaitez accéder à l'interface Internet de Device Manager. Si vous cliquez sur DHCP, le serveur DHCP attribue automatiquement une adresse IP, un masque de sous-réseau et une passerelle par défaut au switch. Tant que le switch n'est pas redémarré, il continue à utiliser les informations IP attribuées et vous êtes en mesure d'utiliser la même adresse IP pour accéder à l'interface Internet de Device Manager. Si vous attribuez manuellement l'adresse IP du switch et que votre réseau utilise un serveur DHCP, assurez-vous que l'adresse IP que vous donnez au switch ne se trouve pas dans la plage d'adresses que le serveur DHCP attribue automatiquement à d'autres dispositifs. Cela empêche les conflits d'adresse IP entre le switch et un autre dispositif.

Champ	Description
IP Address	L'adresse IP et le masque de sous-réseau associé sont des identificateurs uniques pour le switch dans un réseau : • L'adresse IP est une adresse numérique de 32 bits écrite sous forme de quatre nombres séparés par des points. Chaque nombre peut être compris entre 0 et 255. • Le masque de sous-réseau est l'adresse réseau qui identifie le sous-réseau auquel appartient le switch. Les sous-réseaux sont utilisés pour segmenter les dispositifs d'un réseau en groupes plus petits. La valeur par défaut est 255.255.255.0. Ce champ est activé uniquement si le mode d'attribution IP est statique. Assurez-vous que l'adresse IP que vous attribuez au switch n'est pas utilisée par un autre dispositif dans votre réseau. L'adresse IP et la passerelle par défaut ne peuvent pas être les mêmes.
Default Gateway (passerelle par défaut – en option)	L'adresse IP par défaut pour la passerelle. Une passerelle est un routeur ou un dispositif réseau dédié qui permet au switch de communiquer avec les dispositifs dans d'autres réseaux ou sous-réseaux. L'adresse IP de passerelle par défaut doit faire partie du même sous-réseau que l'adresse IP du switch. L'adresse IP du switch et l'adresse IP de la passerelle par défaut ne peuvent pas être les mêmes. Si tous vos dispositifs sont dans le même réseau et qu'une passerelle par défaut n'est pas utilisée, vous n'avez pas besoin d'entrer une adresse IP dans ce champ. Ce champ est activé uniquement si le mode d'attribution IP est statique. Vous devez spécifier une passerelle par défaut si votre station de gestion de réseau et le switch se trouvent dans des réseaux ou sous-réseaux différents. Dans le cas contraire, le switch et la station de gestion de votre réseau ne peuvent pas communiquer entre eux.
NTP Server (serveur NTP)	L'adresse IP du serveur NTP (Network Time Protocol). NTP est un protocole réseau pour la synchronisation d'horloge entre les systèmes d'ordinateur sur des réseaux de données à commutation de paquets et à latence variable.
Réglages avancés	
CIP VLAN	Le VLAN sur lequel le protocole CIP (Common Industrial Protocol) est activé. Le CIP VLAN peut être le même que le VLAN de gestion, ou vous pouvez isoler le trafic CIP sur un autre VLAN déjà configuré sur ce dispositif.
IP Address	L'adresse IP et le masque de sous-réseau pour le CIP VLAN si le CIP VLAN est différent du VLAN de gestion. Le format est une adresse numérique de 32 bits écrite sous forme de quatre nombres séparés par des points. Chaque nombre peut être compris entre 0 et 255. Assurez-vous que l'adresse IP que vous affectez à ce dispositif n'est pas utilisée par un autre dispositif sur votre réseau.
Same As Management VLAN (identique au VLAN de gestion)	Indique si les réglages pour le CIP VLAN sont les mêmes que pour le VLAN de gestion.
Telnet, CIP and Enable Password (et mot de passe de validation – en option)	Le mot de passe utilisé pour la sécurité Telnet et CIP.
Confirm Password (confirmation de mot de passe)	Le même mot de passe que ci-dessus.

Gestion des utilisateurs

Pour ajouter, modifier ou supprimer des utilisateurs et des informations d'ouverture de session utilisateur pour le switch, dans le menu Admin, choisissez Users (utilisateurs).



Vous pouvez spécifier les informations correspondant à chaque utilisateur dans le tableau ci-dessous.

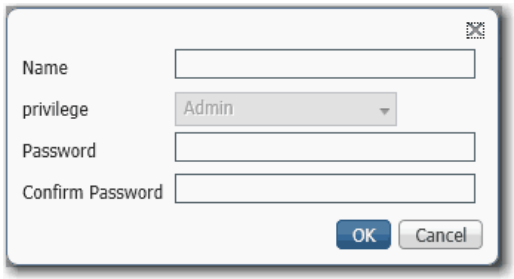


Tableau 22 - Champs d'ajout d'utilisateur

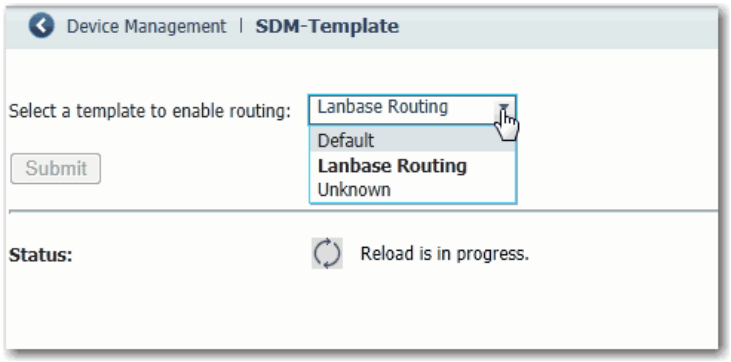
Champ	Description
Name (nom)	Le nom d'utilisateur pour cet utilisateur.
Privilege (privilège)	Le niveau d'accès pour cet utilisateur. Le privilège Admin est affecté à tous les utilisateurs et ils peuvent tous modifier l'ensemble des paramètres.
Password (mot de passe)	Le mot de passe qui est requis pour l'accès avec ce nom d'utilisateur.
Confirm Password (confirmation du mot de passe)	Le même mot de passe que ci-dessus.

Réaffectation de la mémoire du switch pour le routage

Les modèles de gestion de base de données (SDM) optimisent la manière dont la mémoire du switch est affectée à des fonctionnalités spécifiques, telles que le routage. Pour activer le routage, vous devez configurer le modèle Lanbase Routing comme modèle SDM par défaut.

Pour appliquer un modèle SDM, suivez les étapes ci-après.

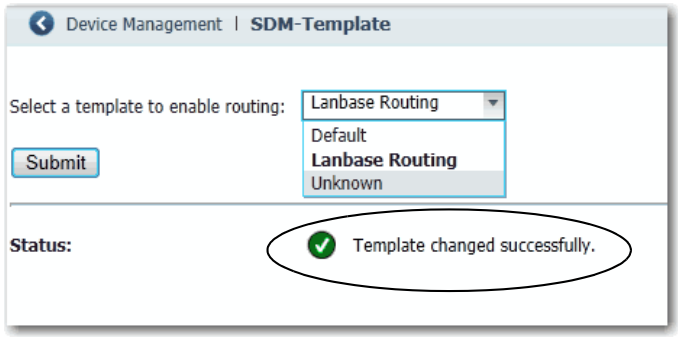
1. Dans le menu Admin, choisissez SDM Template (modèle SDM).
2. Choisissez un modèle dans le menu déroulant :
   - Default : équilibre toutes les fonctions de couche 2
   - Lanbase Routing : maximise les ressources système pour le routage en envoi individuel IPv4, nécessaire pour activer le routage
   - Unknown : configuré par l'utilisateur à partir du CLI



3. Cliquez sur Submit (soumettre).
4. Lorsqu'un message s'affiche pour vous inviter à continuer, cliquez sur OK.

IMPORTANT Le processus de changement du modèle entraîne le redémarrage automatique du switch.

Un message s'affiche une fois le processus terminé.



5. Pour activer le routage, passez au paragraphe Activation et configuration du routage à la page 124.

Redémarrage du switch

Redémarrer ou réinitialiser le switch interrompt la connexion de vos dispositifs au réseau.

Pour redémarrer ou réinitialiser le switch, dans le menu Admin, choisissez Restart/Reset (redémarrer/réinitialiser).

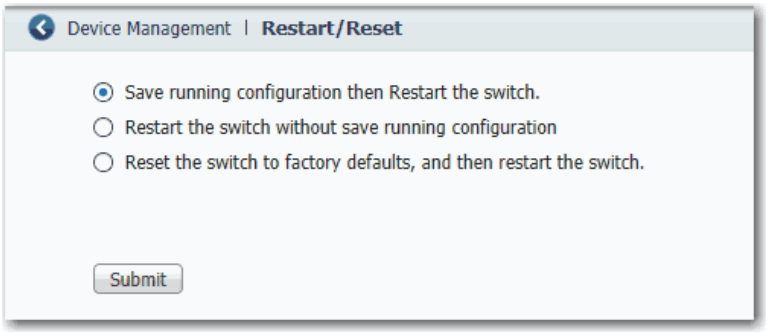


Tableau 23 - Champs Restart/Reset

Champ	Description
Save running configuration and then restart the switch.	Garantit que toutes les modifications dans la configuration en cours d'exécution sont sauvegardées avant le redémarrage du switch.
Restart the switch without saving running configuration.	Redémarre le switch avec les paramètres de configuration enregistrés précédemment.
Reset the switch to factory defaults, and then restart the switch.	Réinitialise le dispositif aux réglages d'usine par défaut, en supprimant les réglages de configuration actuels, puis redémarre le dispositif. Vous perdrez la connectivité avec le dispositif et devrez lancer Express Setup pour reconfigurer le dispositif.

Mise à niveau du firmware du switch

Vous devez avoir accès à Internet pour télécharger le firmware du switch depuis http://www.rockwellautomation.com sur votre ordinateur ou lecteur réseau.

Pour mettre à jour le switch avec les dernières modifications et fonctionnalités, dans le menu Admin, choisissez Software Update(mise à jour logicielle).

Dans l'interface Internet de Device Manager, vous pouvez mettre à niveau vos switchs les uns après les autres.

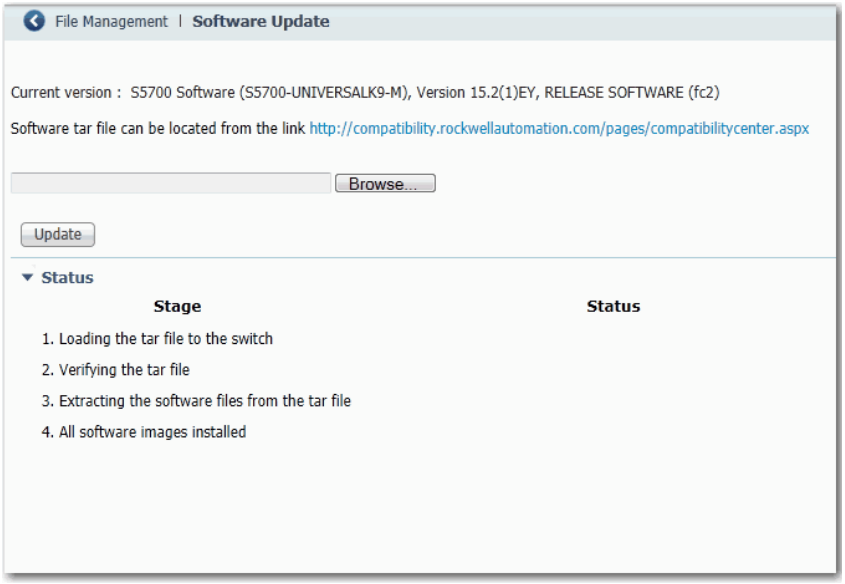
Avec la révision de firmware 2.001 ou ultérieure, la mise à niveau du firmware est installée à l'emplacement de la mémoire non volatile en cours d'exécution :

- Si vous démarrez le switch avec la carte SD insérée, la mise à niveau est installée sur la carte SD.
- Si vous démarrez le switch depuis la mémoire embarquée sans la carte SD insérée, la mise à niveau est installée dans la mémoire flash embarquée.

IMPORTANT Attendez que le processus de mise à niveau se termine. Évitez d'utiliser ou de fermer la session de navigation lorsque l'interface Internet de Device Manager est active. Évitez d'accéder à l'interface Internet de Device Manager à partir d'une autre session de navigateur.

Lorsque le processus de mise à niveau est terminé, un message de réussite apparaît, puis le switch redémarre automatiquement. Avec le nouveau firmware, il est possible que le redémarrage du switch prenne quelques minutes.

Vérifiez que la dernière révision de firmware sur le switch s'affiche dans le champ Software (logiciel) dans la zone Switch Information du tableau de bord.



Pour plus d'informations sur les procédures à suivre, consultez l'aide en ligne de l'interface Internet de Device Manager.

Utilisation de la carte SD pour synchroniser les fichiers de configuration ou IOS

Utilisez la fenêtre Sync pour synchroniser la carte SD avec la mémoire embarquée. Dans l'onglet Manual Sync, vous pouvez consulter les éléments suivants :

- La présence ou non d'une carte
- L'état de la carte
- Si une carte est présente, la source à partir de laquelle le switch a été démarré

Vous pouvez choisir de synchroniser la configuration ou l'IOS du logiciel de la carte SD vers la mémoire embarquée ou de la mémoire embarquée vers la carte SD.

IMPORTANT Vous pouvez écraser votre configuration si vous synchronisez dans la mauvaise direction.

L'onglet Auto Sync vous permet de configurer les options par défaut pour la manière dont l'interface Internet de Device Manager envoie une invite à l'utilisateur après un changement de configuration ou une mise à jour d'IOS.

Pour afficher cette fenêtre, dans le menu Admin, choisissez Sync.

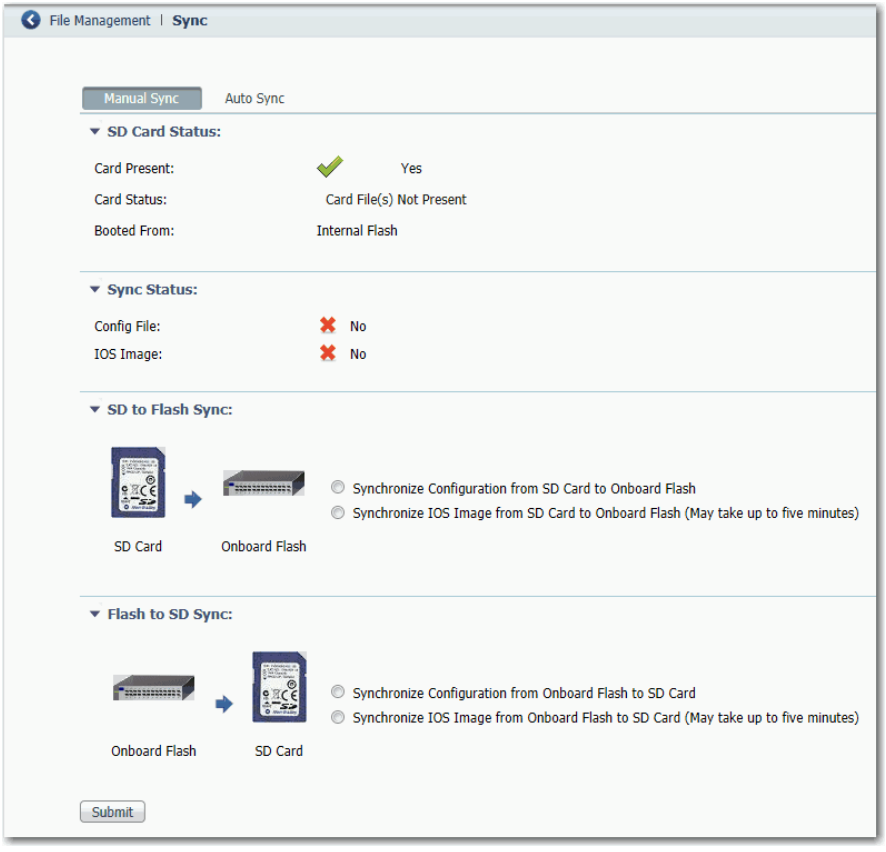


Tableau 24 - Champs de l'onglet Manual Sync

Champ	Description
SD Card Status (état de la carte SD)	Indique si la carte SD est présente, l'état de la carte et d'où sa configuration a été démarrée.
SD to Flash Sync (SD vers Flash Sync)	Choisissez parmi les options suivantes : • Synchroniser la configuration de la carte SD vers la mémoire flash embarquée • Synchroniser l'image IOS de la carte SD vers la mémoire flash embarquée
Flash to SD Sync (Flash vers SD Sync)	Choisissez parmi les options suivantes : • Synchroniser la configuration de la mémoire flash embarquée vers la carte SD • Synchroniser l'image IOS de la mémoire flash embarquée vers la carte SD

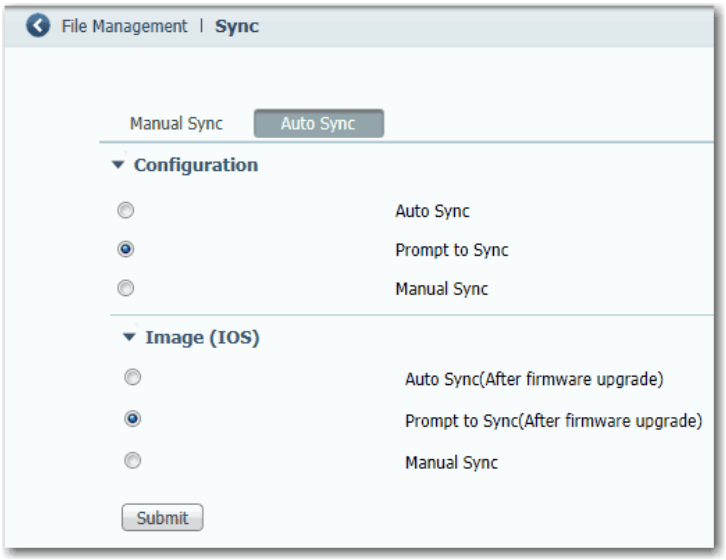


Tableau 25 - Champs de l'onglet Auto Sync

Champ	Description
Configuration	Auto Sync : synchroniser automatiquement la configuration lorsqu'une modification de configuration est faite dans l'interface Internet de Device Manager. C'est la configuration par défaut.
	Prompt to Sync : après qu'un utilisateur a soumis une modification de configuration, l'utilisateur reçoit un message l'invitant à confirmer la synchronisation.
	Manual Sync : aucune synchronisation ne se produit en cas de changement de configuration, sauf si l'utilisateur effectue une synchronisation manuellement.
Image (IOS)	Auto Sync (après mise à niveau du firmware) : synchroniser automatiquement la configuration modifiée une fois le firmware mis à niveau.
	Prompt to Sync (après mise à niveau) : après que le firmware est mis à niveau, l'utilisateur reçoit un message l'invitant à confirmer la configuration. C'est la configuration par défaut.
	Manual Sync : aucune synchronisation ne se produit une fois le firmware mis à niveau, sauf si l'utilisateur effectue une synchronisation manuellement.

Téléchargement des fichiers de configuration

Pour copier un fichier de configuration à partir d'un fichier sur un autre dispositif, comme un PC, vers la mémoire embarquée, entrez le nom du répertoire du dossier sur le switch, parcourez pour sélectionner le fichier, puis cliquez sur Upload (transférer).

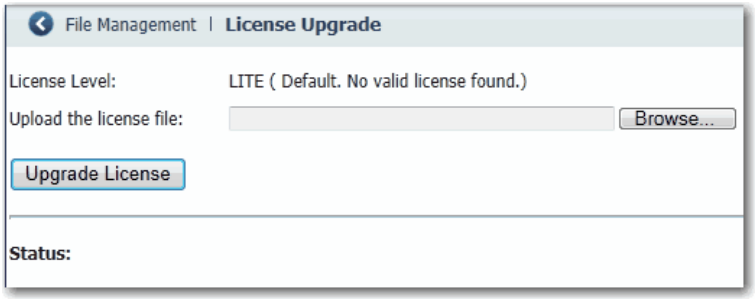
Pour télécharger un fichier de configuration de la mémoire embarquée vers votre ordinateur, faites un clic droit sur le lien, puis choisissez Save Link As (enregistrer le lien sous).

Mise à niveau des fichiers de licence

Après l'obtention d'un fichier de licence, utilisez la fenêtre License Upgrade (mise à niveau de licence) pour l'installer sur le switch.

1. Cliquez sur Browse (parcourir) pour sélectionner le fichier de licence.
2. Cliquez sur Upgrade License (mise à niveau de licence) pour commencer le processus de mise à niveau.

   Des messages s'affichent pour indiquer la progression. Une fois la mise à niveau terminée, le switch redémarre.



Notes :

Gestion du switch via l'environnement Studio 5000

Après avoir terminé Express Setup, vous pouvez gérer le switch à l'aide de l'application Logix Designer dans l'environnement Studio 5000.

Interface CIP EtherNet/IP

Les switchs Stratix 5700 contiennent une interface de réseau EtherNet/IP. Le réseau EtherNet/IP est une spécification de réseau d'automatisation industrielle gérée par l'Open DeviceNet Vendor Association (ODVA). Il utilise le protocole industriel commun (CIP) pour sa couche d'application et l'interface UDP/TCP/IP pour ses couches de transport et de réseau. Cette interface est accessible via les ports Ethernet du switch à l'aide de l'adresse IP du switch.

Connexions réseau CIP

CIP est un protocole de connexion orienté objet, qui prend en charge deux types fondamentaux de messagerie : les connexions implicites et explicites (E/S). Un maximum de 32 connexions est disponible. Les deux types de connexion doivent utiliser le mot de passe du switch avant de pouvoir définir des paramètres du switch. Le mot de passe est le même que celui que vous entrez pendant Express Setup.

Tableau 26 - Connexions réseau CIP

Connexion	Description
Messagerie Explicite	Les connexions de messagerie explicite fournissent des chemins de communication génériques et polyvalents entre deux dispositifs. Ces connexions sont souvent désignées comme des connexions de messagerie. Les messages explicites fournissent une communication réseau orientée selon le schéma demande/réponse-. Chaque requête correspond généralement à un élément de données spécifique. Les messages explicites peuvent être utilisés pour la configuration, la surveillance et le dépannage du switch. L'interface de Messagerie Explicite est utilisée par l'application Logix Designer.
E/S (messagerie implicite)	Les connexions d'E/S fournissent des chemins de communication spécifiques, dédiés entre une application productrice et une ou plusieurs applications consommatrices. Les données d'E/S spécifiques à l'application qui se déplace à travers ces connexions sont typiquement des structures fixes, cycliques. Le switch prend en charge deux choix de connexions E/S. • Input Only (entrée seule) • Exclusive Owner (propiétaire exclusif) Les deux connexions sont cycliques et réglables de 300... 5000 ms. La connexion Input Only (entrée seule) contient une structure de données avec des informations d'état du switch, ainsi que l'état général et spécifique de chacun des ports. Cette connexion est en multidiffusion et peut être partagée par plusieurs automates (initiateurs de connexion). La connexion Exclusive Owner (propiétaire exclusif) utilise la même structure de données d'entrée que la connexion Input only, mais s'y ajoute une structure de données de sortie. Les données de sortie contiennent un bit pour chaque port qui vous permet d'activer ou de désactiver chaque port séparément. Même si les données d'entrée sur cette connexion peuvent être partagées (via la multidiffusion) par de plusieurs automates, un seul automate peut posséder les données de sortie. Si un deuxième automate tente d'ouvrir cette connexion, la connexion est rejetée.

IMPORTANT Étant donné que les données de sortie sont envoyées à l'automate de manière cyclique, elles remplacent toute autre tentative d'activation ou de désactivation d'un port à partir d'autres outils logiciels ou de stations de visualisation.

Logiciel RSLinx et prise en charge de Network Who

L'interface de réseau EtherNet/IP prend également en charge la commande List Identity utilisée par les outils de réseau basés sur CIP, tels que la fonction RSWho du logiciel RSLinx®. RSWho permet de localiser et d'identifier votre switch sur le réseau en utilisant des fichiers de fiches de données électroniques (EDS).

Pour accéder à la fonction RSWho, à partir de la barre d'outils du logiciel RSLinx, choisissez Communications > RSWho.

IMPORTANT Après avoir utilisé la fonction RSWho, si vous accédez au switch et visualisez les compteurs de liaisons Ethernet, vous voyez les informations concernant le premier port uniquement (Port Gi1/1).

Fiches de données électroniques (EDS)

Les fichiers de données électroniques (EDS) sont des fichiers texte utilisés par les outils de configuration de réseau, tels que le logiciel RSNetWorx™ for Ethernet/IP, pour vous aider à identifier les produits et à les mettre en service facilement. Les fichiers EDS contiennent des détails sur les paramètres lisibles et configurables du dispositif. Ils fournissent également des informations sur les connexions d'E/S compatibles avec le dispositif et le contenu des structures de données associées.

Si vous utilisez un switch dans un système qui ne dispose pas d'un automate de type Logix Rockwell Automation pour surveiller ou contrôler votre switch, vous ne pouvez pas utiliser l'AOP fournie avec les automates Logix. Vous devez utiliser des informations provenant des fichiers EDS pour mettre en place la connexion d'E/S.

Le serveur OPC contenu dans le logiciel RSLinx Classic utilise également les fichiers EDS pour vous fournir une liste de paramètres lors de l'ajout d'éléments (points OPC) à une Rubrique (le switch).

Les fichiers EDS pour les switchs Stratix 5700 sont inclus avec les logiciels suivants :

- Logiciel RSLinx, version 2.54 ou ultérieure
- Logiciel RSLogix 5000, version 16 ou ultérieure, ou l'application Logix Designer, version 21.00.00 ou ultérieure
- Logiciel RSNetWorx for EtherNet/IP, version 9.0 ou ultérieure

Vous pouvez également obtenir les fichiers EDS de l'une ou l'autre de ces manières :

- À partir de http://www.rockwellautomation.com/resources/eds/.

  CONSEIL Pour localiser un fichier EDS spécifique, procédez comme suit :
  - Choisissez EtherNet/IP dans le champ Network type.
  - Saisissez Stratix 5700 dans le champ Keyword (mot clé).
  - Laissez les entrées par défaut des autres champs.

- À partir du switch, à l'aide de l'utilitaire d'installation de matériel RSLinx EDS.

Pour télécharger les fichiers EDS directement à partir du switch sur le réseau, procédez comme suit.

1. Dans le menu Démarrer, choisissez Programmes > Rockwell Software > RSLinx >Tools > EDS Hardware Installation Tool.
2. Cliquez sur Add (ajouter) pour lancer l'Assistant EDS et ajoutez la description du matériel sélectionné et les fichiers associés.

Données accessibles via CIP

L'interface CIP vous permet d'accéder aux informations suivantes :

- Données d'entrée via la connexion E/S
  - État de la liaison par port : non connecté, connecté
  - Dispositif non autorisé par port : OK, non OK
  - Seuil d'envoi individuel dépassé par port : OK, dépassé
  - Seuil multidiffusion dépassé sur chaque port : OK, dépassé
  - Seuil diffusion générale dépassé sur chaque port : OK, dépassé
  - Utilisation de bande passante du port par port : valeur en %
  - Relais d'alarme majeure : OK, déclenché
  - Groupes de multidiffusion actifs : quantité
- Données de sortie via la connexion E/S
  - Désactivation de port par port : activé, désactivé
- Autres données d'état
  - Température interne du switch : degrés centigrades
  - Alimentation A présente : oui, non
  - Alimentation B présente : oui, non
  - Informations sur l'identité : ID fournisseur, type de dispositif, code produit, nom produit, révision, numéro de série
  - Version IOS
  - Durée de disponibilité du switch depuis le dernier redémarrage
  - Utilisation de la CPU de gestion : en pourcentage
  - Compteurs de connexion CIP : demandes d'ouverture/fermeture, refus d'ouverture/fermeture, timeouts
  - État d'alarme de port par port : OK, aucun transfert, aucun fonctionnement, erreurs FCS excessives
  - État des défauts de port par port : désactivation d'erreur, erreur SFP, incompatibilité VLAN native, condition du volet Adresse MAC, violation de la sécurité
  - Compteurs de diagnostic port par port : Compteurs d'interface Ethernet (10), compteurs de médias Ethernet (12)

- Données de configuration (nécessite un mot de passe)
  - Méthode de l'adresse IP : DHCP, statique
  - Adresse IP, masque de sous-réseau, passerelle par défaut (toutes si statique)
  - Nom d'hôte
  - Nom de contact
  - Emplacement géographique
  - Configuration du port par port : activer/désactiver, négociation automatique, vitesse/duplex forcée
  - ID MAC autorisée par port
  - Seuil de limitation taux d'envoi individuel par port : en paquets par seconde, en bits par seconde, ou en pourcentage
  - Seuil de limitation taux de multidiffusion : en paquets par seconde, en bits par seconde, ou en pourcentage
  - Seuil de limitation taux de diffusion générale : en paquets par seconde, en bits par seconde, ou en pourcentage
- Attribution SmartPort par port : rôle et VLAN
- Sauvegarde et restauration de la configuration du switch (via Fichier Obj)

Ajout d'un switch à l'arborescence de configuration d'E/S

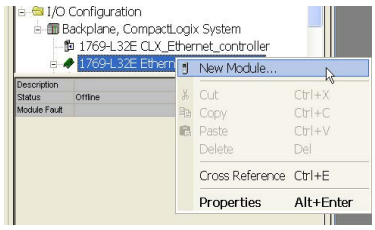
Pour ajouter le switch à l'arborescence des E/S de l'automate, suivez ces étapes.

IMPORTANT Ces étapes sont nécessaires avant de pouvoir configurer et surveiller le switch en ligne.

1. Ouvrez le fichier de projet pour l'automate qui surveille le switch.
2. Sélectionnez le module Ethernet via lequel l'automate communique avec le switch.

   Dans cet exemple, le switch communique via un automate CompactLogix EtherNet/IP 1769-L32E.

3. Faites un clic droit sur le port Ethernet que vous avez créé et choisissez New Module (nouveau module).



4. Cliquez sur Communications.

5. Cliquez sur le signe + et faites défiler vers le bas jusqu'à ce que vous aperceviez le switch que vous souhaitez configurer.

   Si vous ne voyez pas le switch dans la liste, vous pouvez obtenir l'AOP à partir du site Internet d'assistance de Rockwell Automation.

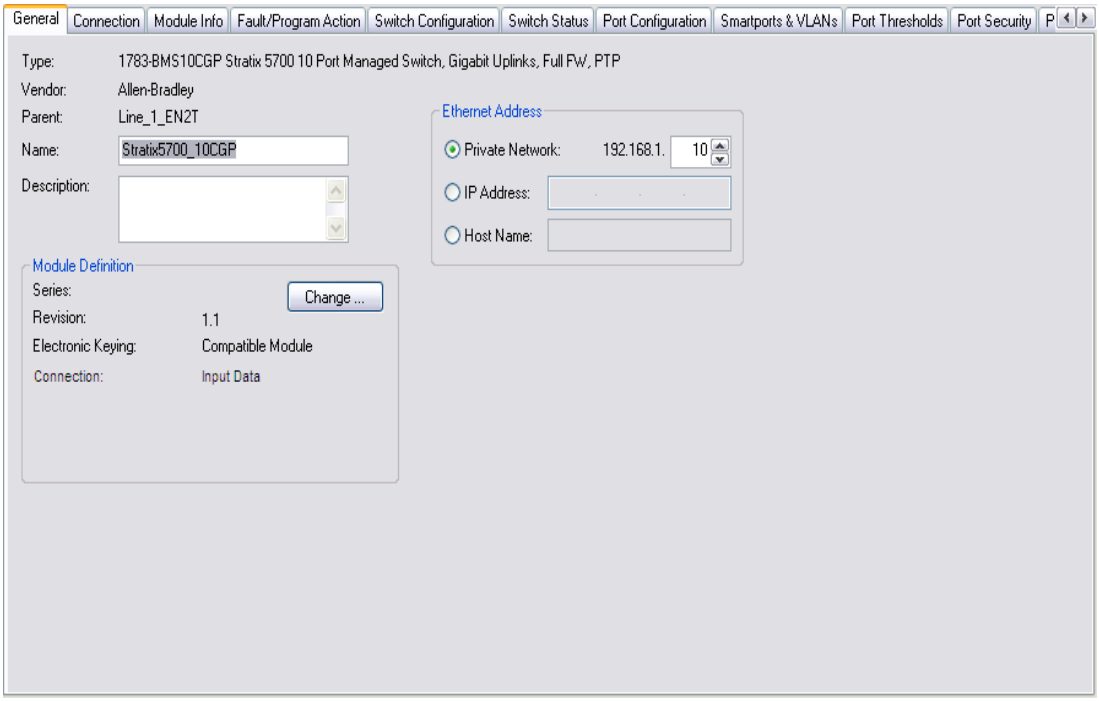
   a. Allez à l'adresse http://www.rockwellautomation.com/support/.

   b. Cliquez sur Downloads/RSLogix 5000 I/O Modules Add-on Profiles.

   c. Choisissez 1783-Stratix 5700 Managed Switches Add-on Profile.

6. Cliquez sur OK pour afficher la boîte de dialogue des propriétés du module.

Configuration des propriétés générales



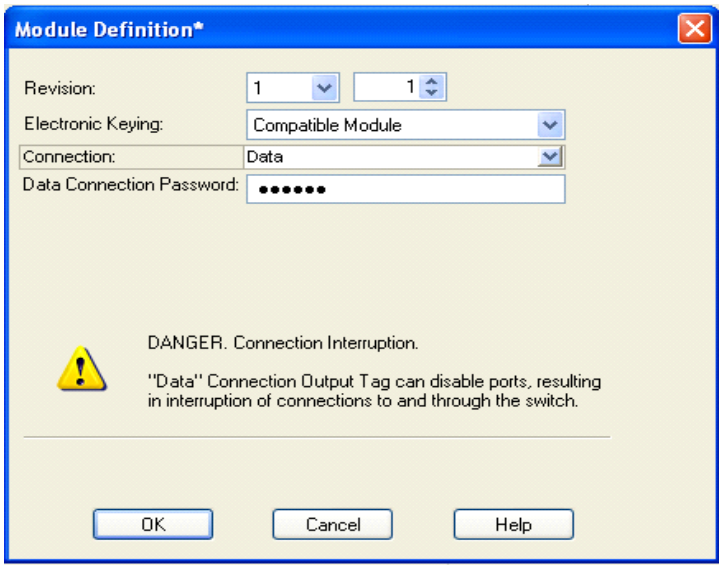
Pour configurer les propriétés générales, procédez comme suit.

1. Dans la boîte de dialogue Module Properties (propriétés du module), renseignez les champs ci-dessous.

Champ	Description
Name (nom)	Le nom que vous choisissez pour le switch.
Description	Une description qui vous aide à vous souvenir de quelque chose d'important concernant le switch.
Ethernet Address (adresse Ethernet)	Choisir parmi les options suivantes : • Private Network - le réseau privé sur lequel se trouve le switch. • IP Address - l'adresse IP que vous avez saisie lorsque vous avez exécuté Express Setup. L'automate utilise l'adresse IP pour communiquer. • Host Name - le nom d'hôte fourni à la configuration initiale lorsque vous avez exécuté Express Setup. Le nom d'hôte requiert que vous disposiez d'un serveur DNS configuré sur le réseau pour le module d'interface Ethernet de l'automate. **IMPORTANT :** assurez-vous que le nom d'hôte et l'adresse IP sont les mêmes que ceux fournis lorsque vous avez exécuté Express Setup.

2. Cliquez sur OK.

3. Mettez le switch en ligne en choisissant Communications > Go online (passer en ligne).
4. Double-cliquez sur le switch pour afficher la boîte de dialogue Module Properties (propriétés du module).
5. Cliquez sur Change (modifier).
6. Renseignez les champs de la boîte de dialogue de Module Definition (définition du module).



Champ	Description
Revision (révision)	La révision majeure et mineure du switch : • Major revision : un nombre compris entre 1 et 128 • Minor revision : un nombre compris entre 1 et 255
Electronic Keying (détrompage électronique)	• Compatible Module (module compatible – par défaut) • Exact Match (correspondance exacte) • Disable Keying (détrompage désativé)
Connection (connexion)	• Input Data (données d'entrée – par défaut) : active uniquement la connexion de données d'entrée • Data : active la connexion de données d'entrée et de sortie **ATTENTION :** cette sélection active les points de sortie, qui peuvent désactiver les ports et interrompre les connexions vers et par l'intermédiaire du switch. Vous pouvez désactiver un port du switch en définissant le bit correspondant dans le point de sortie. Les bits de sortie sont appliqués chaque fois que le switch reçoit les données de sortie de l'automate lorsque l'automate est en mode Run (Exécution). Lorsque l'automate est en mode Program, les bits de sortie ne sont pas appliqués. Le port est activé si le bit de sortie correspondant est à 0. Si vous activez ou désactivez un port à l'aide de l'interface Internet de Device Manager ou la CLI, le réglage du port peut être écrasé par les bits de sortie de l'automate lors de la mise à jour cyclique suivante de la connexion E/S. Les bits de sortie ont toujours la priorité, peu importe si l'interface Internet de Device Manager ou CLI a été utilisée pour activer ou désactiver le port.
Data Connection Password (mot de passe de la connexion de données)	Entrez le mot de passe pour accéder au switch. Nécessaire uniquement pour la connexion Data.

Propriétés de connexion

Vous pouvez définir des propriétés de connexion pour le switch dans l'onglet Connection (connexion).

Tableau 27 - Champs de l'onglet Connexion

Champ	Description
Requested Packet Interval (intervalle entre trames requis – RPI)	Entrez une valeur comprise entre 300 et 5000.
Inhibit Module (inhibition de module)	Cochez pour désactiver la communication entre l'automate et le switch. Décochez la case afin de rétablir la communication.
Major Fault on Controller If Connection Fails While in Run mode	Cochez pour que l'automate crée un défaut majeur si la connexion échoue en mode Run.
Use Unicast Connections over EtherNet/IP	Cochez pour utiliser les connexions d'envoi individuel avec le réseau EtherNet/IP.
Module Fault (défaut de module)	Affiche le code d'erreur retourné par l'automate (lié au switch que vous êtes en train de configurer) et le texte qui détaille la défaillance de module survenue.

Informations sur le module

Vous pouvez surveiller et réinitialiser le switch à partir de l'onglet Module Info.

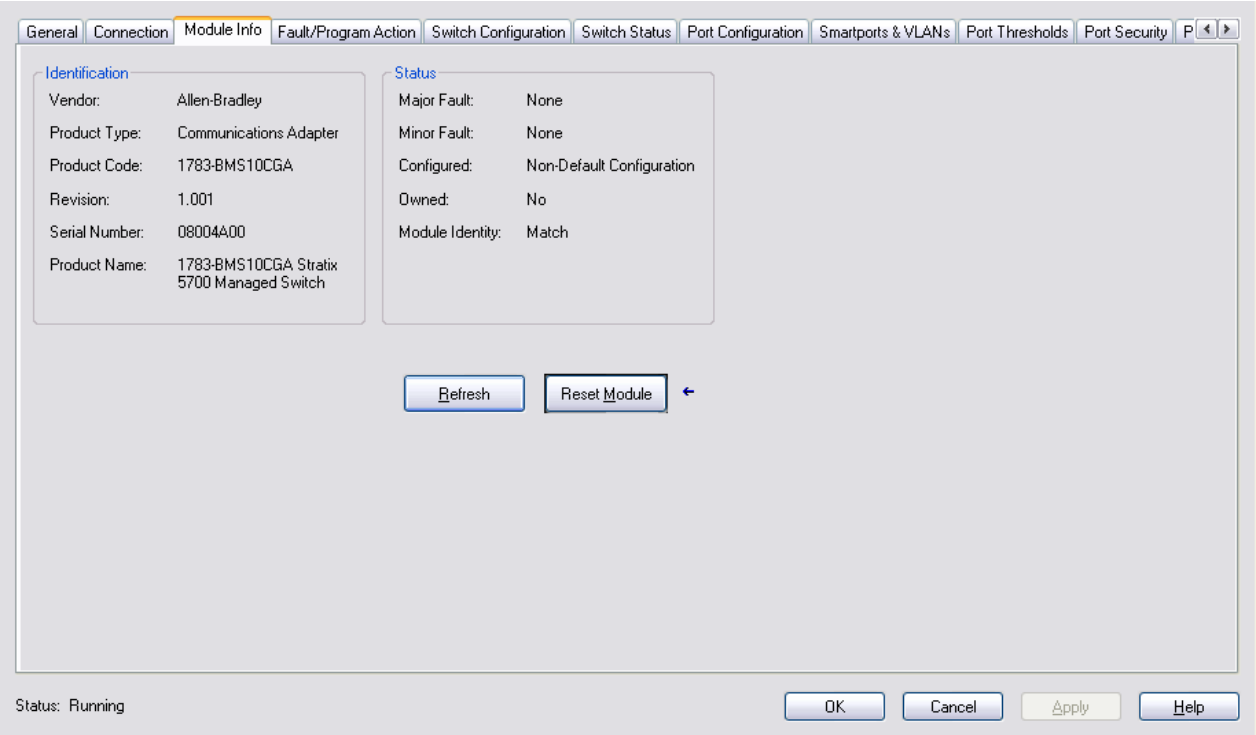


Tableau 28 - Champs de l'onglet Module Info

Champ	Description
Identification	Affiche les informations suivantes à propos du switch : • Vendor (fournisseur) • Product type (type produit) • Product code (code produit) • Revision (version) • Serial number (numéro de série) • Product name (nom de produit)
Status (état)	Affiche l'état des éléments suivants : • État de défaut majeur/mineur : – None (aucun) – Recoverable 'récupérable) – Non-recoverable (irrécupérable) • Configuration : – Non-default configuration (configuration non par défaut) – Default configuration (configuration par défaut) • Owned. (propriété) Indique s'il existe une connexion d'E/S : – Yes (oui) – No (non) • Identité de module : – Match. (correspondance) Coïncide avec ce qui est spécifié dans l'onglet General. Pour que la condition Match existe, il faut que vendor, product type, product code et major revision correspondent. – Mismatch. (discordance) Ne coïncide pas avec ce qui est spécifié à l'onglet General. Le champ Module Identify ne prend pas en compte les sélections Electronic Keying (détrompage électronique) ou Minor Revision (révision mineure) indiquées à l'onglet General pour le switch.
Refresh (rafraîchir)	Cliquez pour actualiser l'onglet avec les nouvelles données provenant du module.
Reset Module (réinitialisation de module)	Cliquez pour effectuer une réinitialisation du switch (mise sous tension) avec le fichier de configuration actuel. La boîte de dialogue de Password Confirmation (confirmation du mot de passe) peut s'afficher. **ATTENTION** : la réinitialisation d'un module entraîne la fermeture de toutes les connexions vers ou via le module. Cela peut entraîner une perte de commande.

Propriétés de configuration du switch

Vous pouvez configurer les réglages IP et les paramètres administratifs à partir de l'onglet Switch Configuration (configuration du switch). Vous devez être en ligne pour procéder à ces configurations. En mode hors ligne, rien ne s'affiche sur cet onglet.

L'adresse IP peut être assignée manuellement (statique) ou automatiquement par un serveur DHCP. La valeur par défaut est Static. Nous vous recommandons d'utiliser Static et d'attribuer manuellement l'adresse IP du switch. Vous pouvez ensuite utiliser la même adresse IP chaque fois que vous souhaitez accéder au switch.

- Static - entrez manuellement l'adresse IP, le masque de sous-réseau et la passerelle.
- DHCP - Le switch obtient automatiquement une adresse IP, une passerelle par défaut et un masque de sous-réseau à partir du serveur DHCP. Tant que le switch n'est pas redémarré, il continue à utiliser les informations IP assignées.

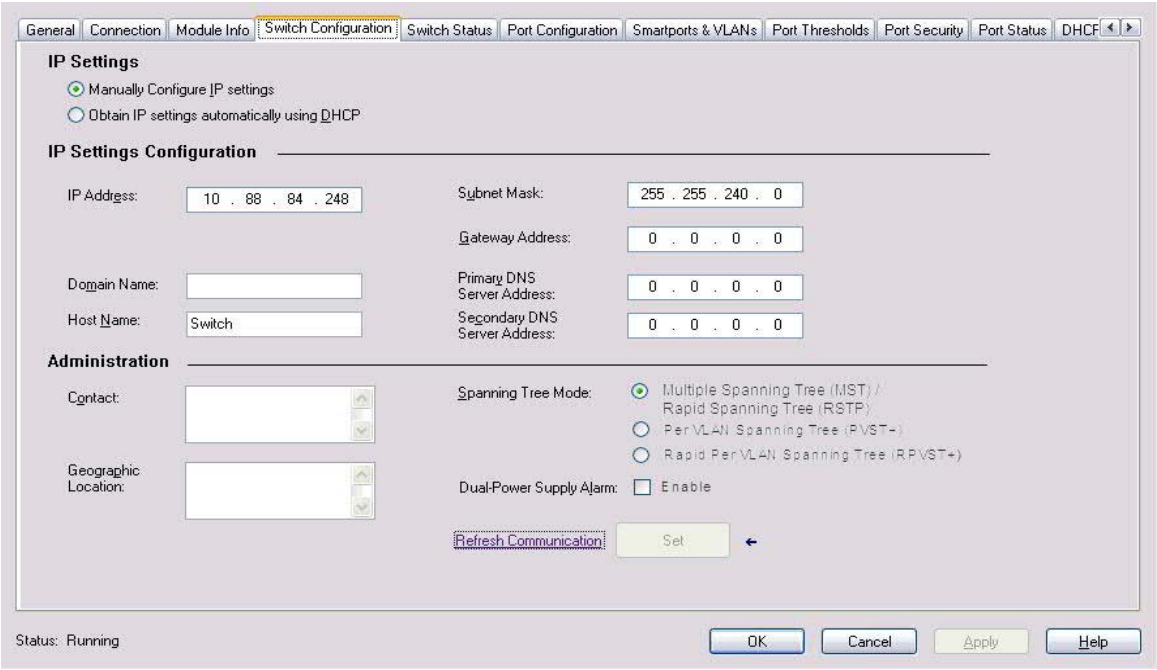


Tableau 29 - Champs de l'onglet Switch Configuration

Champ	Description
IP Address (adresse IP)	Cette valeur doit correspondre à l'adresse IP dans l'onglet General. Si vous reconfigurez votre switch avec une adresse IP différente, vous risquez de perdre la communication avec le switch lorsque vous cliquez sur Set (établir). Pour corriger ce problème, vous devez retourner à Express Setup et à l'onglet General, définir la nouvelle adresse IP et la télécharger dans l'automate.
Subnet Mask (masque de sous-réseau)	Entrez le masque de sous-réseau approprié pour le switch. Le masque de sous-réseau est un nombre de 32 bits. Définissez chaque octet entre 0 et 255. La valeur par défaut est 255.255.255.0.
Gateway Address (adresse de passerelle)	Une passerelle est un routeur ou un autre dispositif réseau via lequel le switch communique avec des dispositifs sur d'autres réseaux ou sous-réseaux. L'adresse IP de la passerelle doit faire partie du même sous-réseau que l'adresse IP du switch. L'adresse IP du switch et l'adresse IP de la passerelle par défaut ne peuvent pas être les mêmes. **IMPORTANT :** la communication est interrompue lorsque vous modifiez l'adresse (IP) de la passerelle.
Primary DNS Server Address (adresse du serveur DNS principal)	Entrez l'adresse IP du serveur DNS principal. Définissez chaque octet entre 0 et 255. Le premier octet ne peut pas être égal à 127 ou supérieur à 223.
Secondary DNS Server Address (adresse de serveur DNS secondaire)	Entrez l'adresse IP du serveur DNS secondaire. Définissez chaque octet entre 0 et 255. Le premier octet ne peut pas être égal à 127 ou supérieur à 223.
Domain Name (nom de domaine)	Entrez le nom du domaine dans lequel réside le module. Le nom de domaine se compose d'une séquence d'étiquettes de nom séparées par des points, par exemple, exemple.com. Le nom de domaine est limité à 48 caractères et aux lettres ASCII a à z, aux chiffres de 0 à 9 et aux points et traits d'union.
Host name (nom d'hôte)	(facultatif). Entrez un nom pour aider à identifier le switch lors de la surveillance ou lors du dépannage d'un problème. Le nom comporte 64 caractères maximum et peut inclure des caractères alphanumériques et spéciaux (virgule et tiret).
Contact	(facultatif). Entrez les informations de contact pour le switch, jusqu'à 200 caractères. Les informations de contact peuvent inclure des caractères alphanumériques et spéciaux (tiret et virgule) et un retour à la ligne.
Geographic Location (emplacement géographique)	(facultatif). Entrez un emplacement géographique pour le switch, jusqu'à 200 caractères. L'emplacement géographique peut inclure des caractères alphanumériques et spéciaux (tiret et virgule) et un retour à la ligne.
Spanning Tree Mode (mode arbre maximal)	Choisir parmi les options suivantes : • RSTP/MST • PVST+ • RPVST+ RSTP/MST est la valeur par défaut.
Dual-Power Supply Alarm (alarme alimentation double)	Cochez la case pour activer la fonctionnalité. La fonctionnalité est désactivée par défaut.
Refresh (actualisation)	Cliquez pour actualiser l'onglet avec les nouvelles données provenant du switch.
Set (établir)	Cliquez pour enregistrer les réglages dans le switch et la carte SD, le cas échéant. Une fois le mot de passe saisi correctement, il est possible de procéder à des changements dans les 10 minutes qui suivent sans que la boîte de dialogue Enter Password ne vous demande un mot de passe.

État du switch

À partir de l'onglet Switch Status, vous pouvez visualiser divers paramètres d'état du switch.

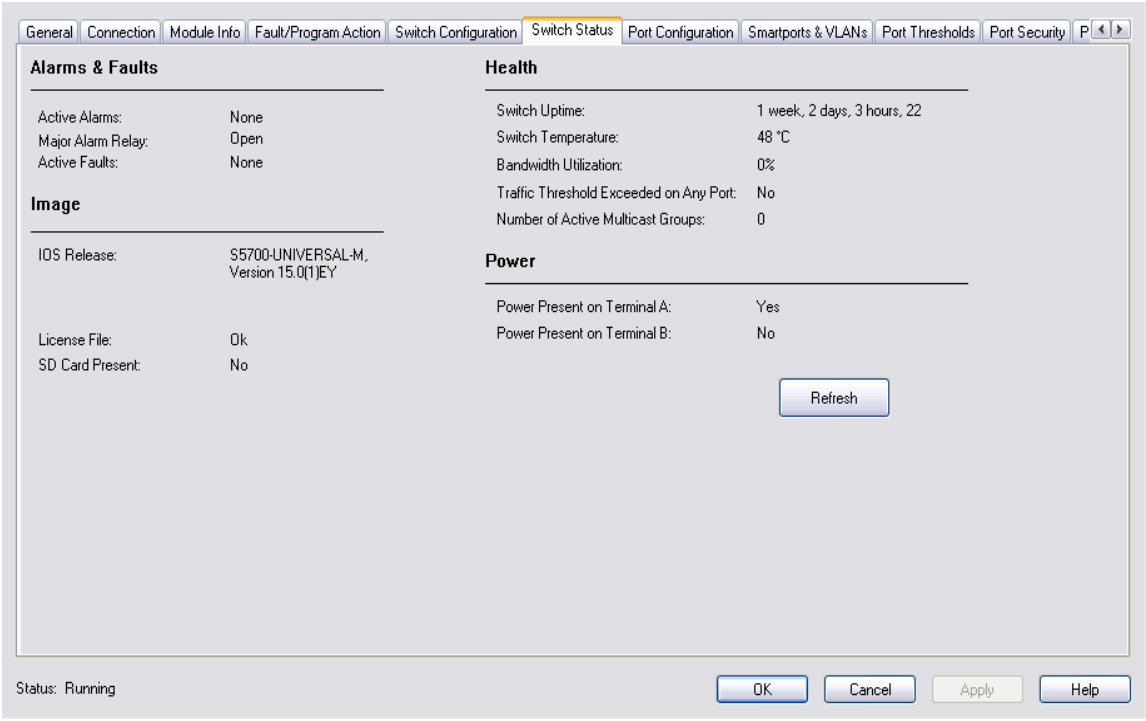


Tableau 30 - Champs de l'onglet Switch Status

Champ	Description
Active Alarms (alarmes actives)	Affiche l'une des valeurs suivantes : • None (aucune) • Port alarm (alarme de port) • Dual Mode Power Supply alarm (alarme de mode alimentation double) • Primary Temperature alarm (alarme de température principale)
Major Alarm Relay (relais d'alarme principale)	Affiche l'une des valeurs suivantes : • Open (ouvert) • Closed (ferm)
Active Faults (défauts actifs)	Affiche l'une des valeurs suivantes : • None (aucun) • Port fault (défaut de port) • Hardware fault (défaut matériel) Si les défauts de matériel et de port sont actifs, l'état de défaut matériel s'affiche.
Traffic Threshold Exceeded on Any Port (seuil de trafic dépassé sur tout port)	Affiche une valeur Oui ou Non indiquant si les seuils actuels d'envoi individuel, multidiffusion ou diffusion générale ont été dépassés sur un port, quel qu'il soit. Pour voir l'état des ports actifs, cliquez sur l'onglet Port Status (état de port). Pour afficher les valeurs de seuil, cliquez sur l'onglet Advanced - Port Threshold (avancé – seuil de port).
Switch Uptime switch en service)	Affiche les jours, les heures et les minutes de fonctionnement du switch depuis le dernier redémarrage.
Switch Temperature (température du switch)	Affiche la température interne actuelle (en degré Celsius) du switch.
Bandwidth Utilization (utilisation de la bande passante)	Affiche le pourcentage total de la bande passante utilisée.
Power Present on Terminal A (alim. présente sur la borne A)	Affiche une valeur Oui ou Non indiquant si une source d'alimentation est présente sur la borne A.
Power Present on Terminal A (alim. présente sur la borne B)	Affiche une valeur Oui ou Non indiquant si une source d'alimentation est présente sur la borne B.
Number of Active Multicast Groups (nbre de groupes multidiffusion actifs)	Affiche le nombre de groupes de multidiffusion actifs.
IOS Release (version IOS)	Affiche la version actuelle du système d'exploitation du switch.

Configuration du port

Les réglages de configuration du port déterminent la façon dont sont reçues et émises les données entre le switch et le dispositif associé.

Vous devez être en ligne pour configurer les fonctionnalités de port. La plupart des informations sur cet onglet ne s'affichent pas si vous êtes en mode hors ligne.

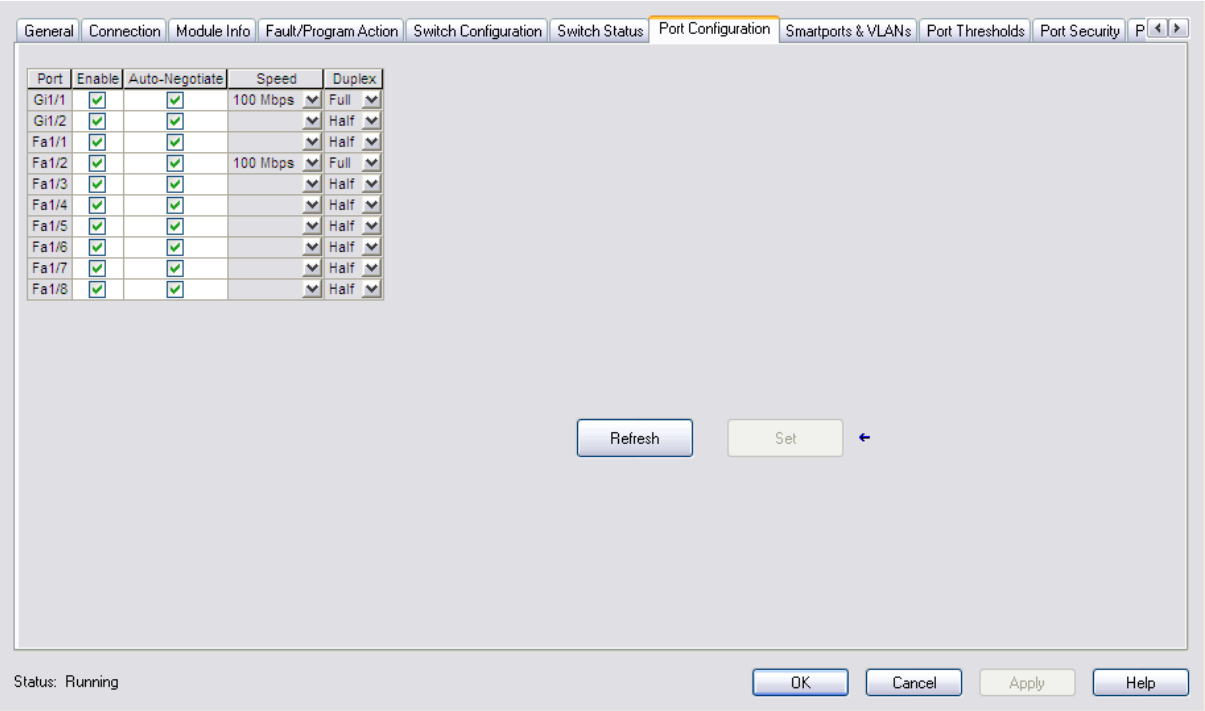


Tableau 31 - Champs de l'onglet Port Configuration

Champ	Description
Port	Le port sélectionné pour la configuration. Le numéro de port inclut le type de port (Fa pour Fast Ethernet et Gi pour Gigabit Ethernet) et le numéro de port spécifique. **EXEMPLE :** Gi1/1 est un port Gigabit Ethernet 1.
Enable (activer)	Cochez la case pour activer le port. Décochez la case pour désactiver manuellement (éteindre) le port. Nous recommandons de désactiver le port si le port n'est pas utilisé et n'est pas relié à un dispositif. Vous pouvez dépanner une connexion présumée non autorisée en désactivant manuellement le port.
Auto-negotiate (auto négociation)	Cochez la case si vous souhaitez que le port et le dispositif terminal procèdent à l'auto négociation de la vitesse de liaison et du mode Duplex. Désactivez la case pour spécifier manuellement la vitesse de port et le mode Duplex désirés. Nous recommandons d'utiliser la valeur par défaut (auto négociation) afin que les réglages de vitesse et de duplex sur le port du switch correspondent automatiquement au réglage du dispositif connecté. Modifiez la vitesse du port et le duplex du switch si le dispositif connecté requiert une vitesse et un duplex spécifiques. Si vous définissez la vitesse et le duplex pour le port du switch, le dispositif connecté doit également être configuré sur les mêmes vitesses et duplex, et ne doit pas être configuré pour l'auto négociation, car cela entraînerait une discordance vitesse/duplex. Les interfaces à fibres optiques ne sont pas compatibles avec l'auto négociation.
Speed (vitesse)	Choisissez la vitesse de fonctionnement du port. Gigabit (Gi) : • 10 Mbits/s • 100 Mbits/s • 1 Gbits/s Fast Ethernet (Fa) : • 10 Mbits/s • 100 Mbits/s
Duplex	Choisir l'un de ces modes Duplex : • Half-duplex : les deux dispositifs ne peuvent pas envoyer de données en même temps. Le mode Half-duplex n'est pas disponible lorsque la vitesse est définie sur 1 Gbits/s. • Full-duplex : les deux dispositifs peuvent envoyer des données en même temps.

Smartports et VLAN

À partir de l'onglet Smartports & VLANs, vous pouvez assigner des rôles smartport et des VLAN aux ports du switch. Vous pouvez également créer, modifier et supprimer des VLAN. Vous devez être en ligne pour configurer ces fonctionnalités de port. La plupart des informations sur cet onglet ne s'affichent pas si vous êtes en mode hors ligne.

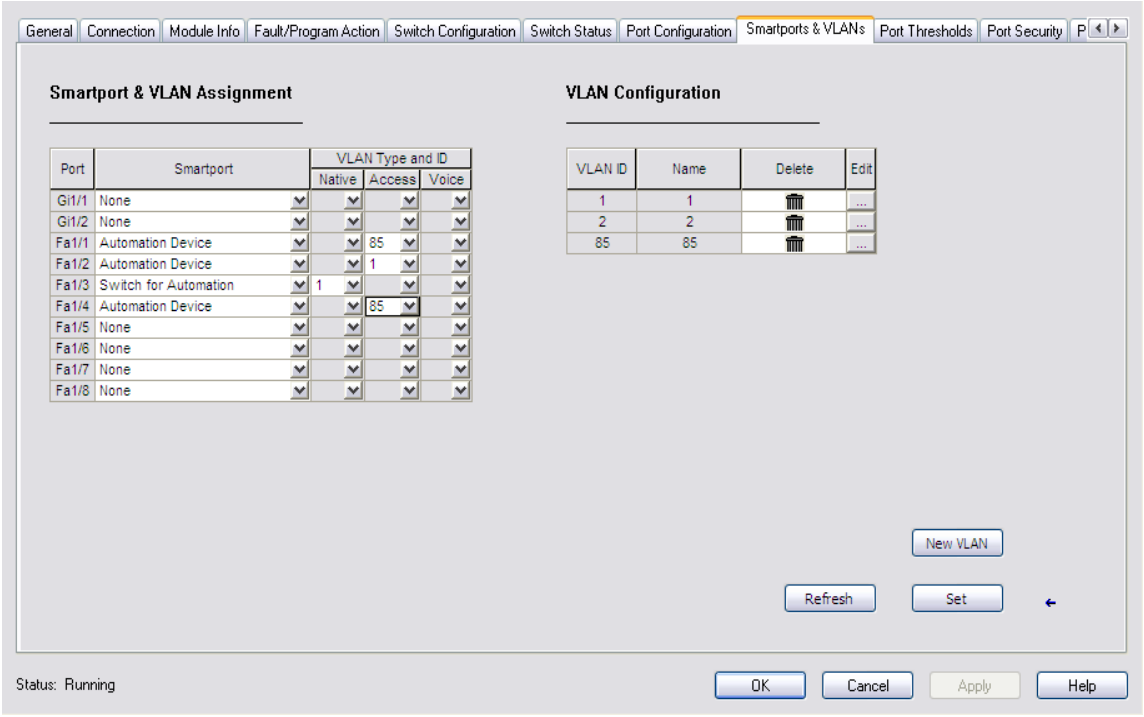


Tableau 32 - Champs de l'onglet Smartports et VLANs

Champ	Description
Port	Le port sélectionné pour la configuration. Le numéro de port inclut le type de port (Fa pour Fast Ethernet et Gi pour Gigabit Ethernet) et le numéro de port spécifique. **EXEMPLE :** Gi1/1 est un port Gigabit Ethernet 1.
SmartPort	Les rôles SmartPort sont des configurations recommandées pour les ports. Ces configurations sont considérées comme des rôles de port. Elles optimisent les connexions du switch et fournissent sécurité, qualité de transmission et fiabilité au trafic depuis les ports du switch. Ces configurations évitent également les nombreux problèmes causés par les erreurs de configuration de port. Les rôles de port se basent sur le type de dispositif connecté au port du switch. Assurez-vous de bien décider quel port est relié à quel type de dispositif avant de choisir un rôle Smartport. Choisissez l'un de ces rôles Smartport à appliquer au port connecté : • Automation Device - Appliquez ce rôle aux ports à connecter aux dispositifs EtherNet/IP. Il peut être utilisé pour les dispositifs d'automatisation industrielle, tels que les automates logiques et des E/S. – Le port est défini sur le mode Access. – La sécurité de port prend en charge un seul MAC ID. – Gestion de la file d'attente optimisée pour le trafic CIP. • Desktop for Automation - Appliquez ce rôle aux ports à connecter à des appareils de bureau, tels que les ordinateurs de bureau, les stations de travail, les ordinateurs portables et autres hôtes basés sur un client. Ce rôle n'est pas adapté aux ports à connecter à des switchs, des routeurs ou des points d'accès. – Le port est défini sur le mode Access. – Portfast activé. – La sécurité de port prend en charge un seul MAC ID. • Switch for Automation - Appliquez ce rôle aux ports à connecter à d'autres switchs. – Le port est défini sur le mode Trunk. – Portfast activé. • Router for Automation - Appliquez ce rôle aux routeurs ou ports à connecter à des switchs Couche 3 avec services de routage activés. • Phone for Automation - Appliquez ce rôle aux ports à connecter à des téléphones IP. Un périphérique de bureau, tel qu'un ordinateur, peut être connecté à un téléphone IP. Le téléphone IP et l'ordinateur connecté ont accès au réseau par l'intermédiaire du port. Ce rôle hiérarchise le trafic téléphonique par rapport au trafic de données général pour fournir une réception téléphonique claire sur les téléphones IP. – Le port est défini sur le mode Trunk. – La sécurité de port prend en charge trois MAC ID vers ce port. • Wireless For Automation - Appliquez ce rôle aux ports à connecter aux points d'accès sans fil. Le point d'accès peut fournir l'accès au réseau à 30 utilisateurs mobiles maximum. • Port-Mirroring - Appliquez ce rôle aux ports devant être surveillés par un analyseur de réseau. Pour plus d'informations concernant cette option, Reportez-vous à Mise en miroir de ports, à la page 92. • None - Appliquez ce rôle aux ports si vous ne souhaitez pas un rôle Smartport spécialisé sur le port. Ce rôle peut être utilisé sur les connexions à tout dispositif, y compris aux dispositifs ayant les rôles décrits ci-dessus. • Custom - Créez ces rôles pour votre application. Vous pouvez définir le type de VLAN qui vous mettez en œuvre, le cas échéant. – Entrez le nom de la macro. Les noms de macro sont sensibles à la casse. La chaîne peut comporter jusqu'à 31 caractères alphanumériques. La chaîne ne peut pas comporter de ?, d'espace ou de tabulation. – Choisir une icône pour la macro (CS1 à CS10).
VLAN Configuration (configuration VLAN)	Affiche le nom et l'ID du VLAN : • VLAN ID - L'identifiant unique (dans une plage allant de 2 à 4 094 ; 1 002 à 1 005 réservés) d'un VLAN, que vous créez en cliquant sur Add New VLAN (ajouter un nouveau VLAN). VLAN ID 1 est la valeur par défaut. • Name - Le nom unique du VLAN (20 caractères maximum) que vous créez en cliquant sur Add New VLAN.

Seuils de ports

Vous pouvez configurer des limites de seuil pour le trafic en diffusion générale, envoi individuel et multidiffusion pour chaque port actif dans l'onglet Port Threshold (seuil de port). Cette fonctionnalité est disponible uniquement avec le firmware complet. Le nombre de paquets envoyés est comparé à la valeur de seuil. Ces limites permettent d'empêcher un dispositif d'envoyer trop de trafic. Pour plus d'informations à propos de cette fonctionnalité, voir Seuils de port à la page 75.

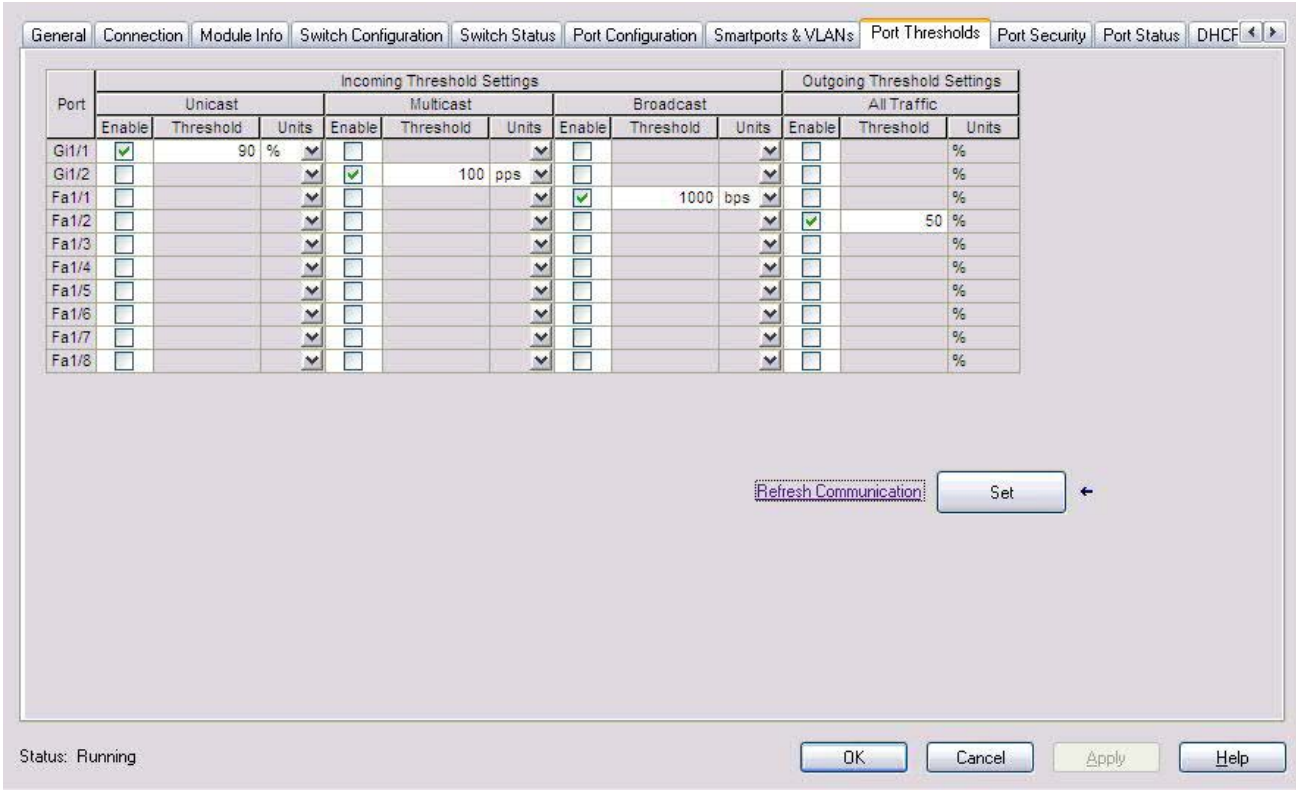


Tableau 33 - Champs de l'onglet Port Threshold

Champ	Description
Port	Le port sélectionné pour la configuration. Le numéro de port inclut le type de port (Fa pour Fast Ethernet et Gi pour Gigabit Ethernet) et le numéro de port spécifique. **EXEMPLE :** Gi1/1 est un port Gigabit Ethernet 1.
Incoming Threshold Settings (réglages de seuil entrant)	Vous permet d'activer des seuils entrants et de définir les valeurs de seuil pour le trafic en envoi individuel, multidiffusion et diffusion générale de chaque port. Valeurs valides pour les unités : • Packets par seconde (pps) • Pourcentage de la bande passante totale (%) • Bits par seconde (bps)
Outgoing Threshold Settings (réglages de seuil sortant)	Vous permet d'activer des seuils sortants et de définir les valeurs de seuil pour le trafic de chaque port. Units % = Pourcentage de la bande passante totale

Sécurité des ports

La fonctionnalité Port Security est valable uniquement pour le firmware complet. Pour plus d'informations, voir Sécurité des ports à la page 77.

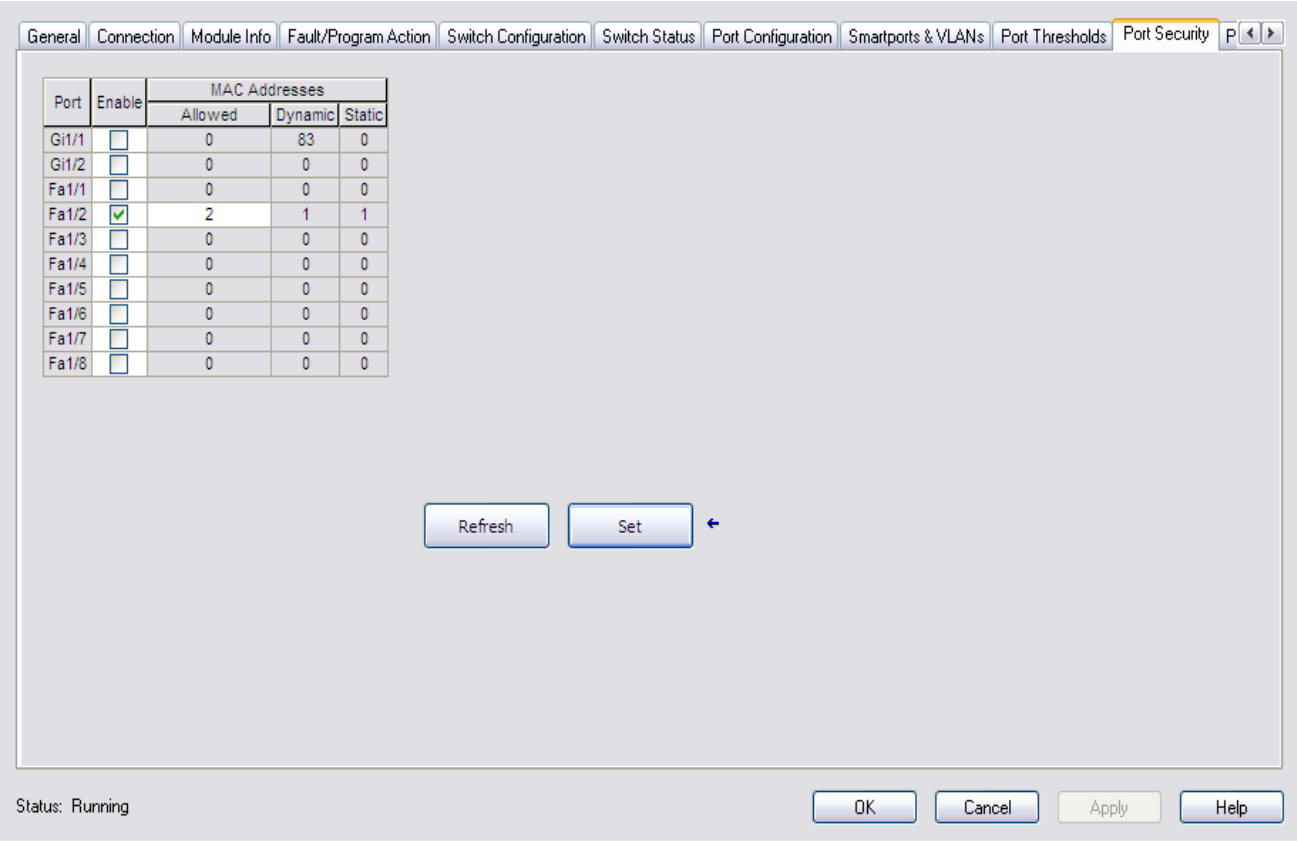


Tableau 34 - Champs de l'onglet Port Security

Champ	Description
Port	Le port sur lequel vous souhaitez activer ou désactiver la sécurité.
Enable (activer)	Cochez la case pour activer la sécurité du port.
MAC Addresses (adresses MAC)	Le nombre d'adresses MAC statiques ou dynamiques prises en charge. • Allowed : 1 à 80. • Dynamic : le nombre d'adresses MAC (dispositifs) actuellement connectées au port qui ne sont pas définies manuellement (statiquement). • Static : le nombre d'adresses MAC (dispositifs) définies statiquement à l'aide de l'interface Internet de Device Manager. Notez que ce nombre doit être supérieur à la somme statique + dynamique pour un port donné. Si vous souhaitez définir un nombre inférieur, débranchez les dispositifs appropriés et laissez leurs entrées dans le timeout du tableau de sécurité du port.

État du port

L'onglet Port Status vous permet de surveiller les alarmes, les états, les seuils et l'utilisation de la bande passante. Vous pouvez également afficher les diagnostics de port et de câble.

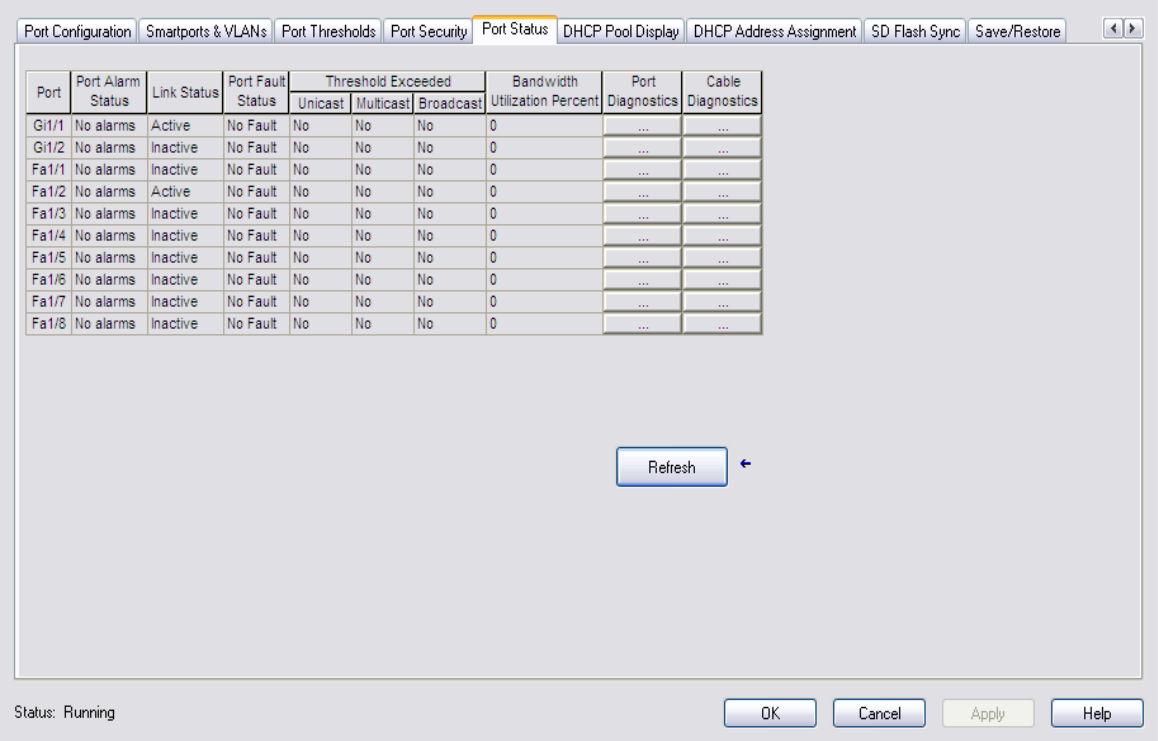


Tableau 35 - Champs de l'onglet Port Status

Champ	Description
Port	Affiche le port sélectionné. Le numéro de port inclut le type de port (Fa pour Fast Ethernet et Gi pour Gigabit Ethernet) et le numéro de port spécifique. **EXEMPLE :** Gi1/1 est un port Gigabit Ethernet 1.
Port Alarm Status (état d'alarme de port)	Affiche l'état actuel de l'alarme de port. Valeurs valides : • Link fault alarm (alarme défaut de liaison) • Port not forwarding alarm (alarme port ne transmet pas) • Port not operating alarm (alarme port hors fonctionnement) • High bit error rate alarm (alarme erreur bit haut) • No alarms (pas d'alarmes)
Link Status (état liaison)	Indique si la liaison est active ou inactive.
Port Fault Status (état défaut de port)	Affiche l'état actuel de l'alarme de port. Valeurs valides : • Error - Disable event (événement de désactivation) • SFP error - Disabled (erreur SFP - désactivée) • CDP native VLAN mismatch (discordance CDP natif VLAN) • MAC address flap (volet adresse MAC) • Port security violation (violation de sécurité du port) • No fault (sans défaut)
Threshold Exceeded (dépassement de seuil)	Affiche les modifications inhabituelles pour ces types de trafic réseau : • Unicast - affiche une valeur Oui ou Non indiquant si le trafic en envoi individuel actuel a dépassé la valeur de seuil. • Multicast - affiche une valeur Oui ou Non indiquant si le trafic en multidiffusion actuel a dépassé la valeur de seuil. • Broadcast - affiche une valeur Oui ou Non indiquant si le trafic en diffusion générale actuel a dépassé la valeur de seuil.
Bandwidth Utilization Percent (pourcentage utilisation bande passante)	Affiche le pourcentage de bande passante utilisée. Veuillez noter que le pourcentage d'utilisation est ce que vous attendez pendant le temps donné d'activité réseau. Si l'utilisation est supérieure à ce qui est prévu, un problème peut exister.
Port Diagnostics (diagnostics de port)	Cliquez pour afficher la boîte de dialogue Port Diagnostics pour le port correspondant. La boîte de dialogue Port Diagnostics vous fournit des informations permettant de diagnostiquer un problème de performances réseau.
Cable Diagnostics (diagnostics de câble)	Cliquez pour afficher la boîte de dialogue Cable Diagnostics pour le port correspondant. La boîte de dialogue Cable Diagnostics fournit des informations permettant de diagnostiquer un problème de câble.

Diagnostics de port

Utilisez la boîte de dialogue Port Diagnostics pour afficher l'état de la performance de la liaison :

- Visualisez les compteurs d'octets et de paquets
- Visualisez les collisions sur la liaison
- Visualisez les erreurs sur la liaison
- Réinitialisez et effacez tous les compteurs d'état

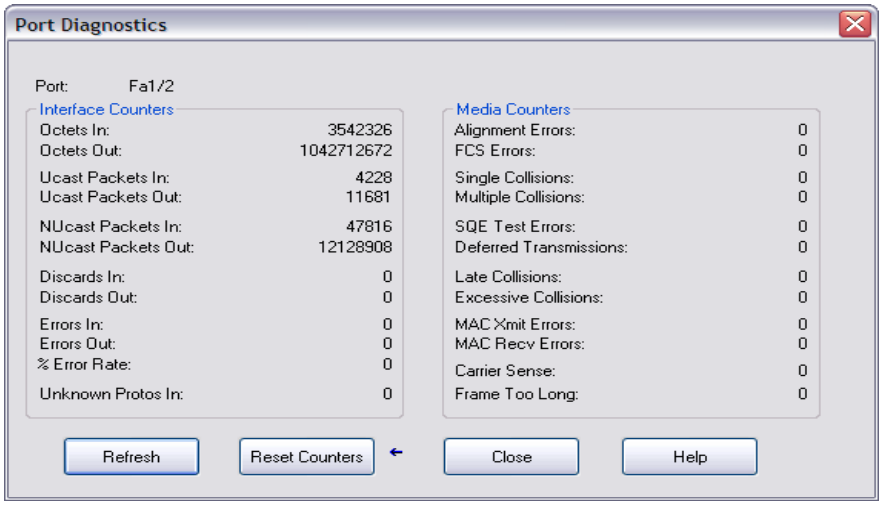


Tableau 36 - Champs de la boîte de dialogue Port Diagnostics

Champ	Description
Port	Le port sélectionné pour la configuration. Le numéro de port inclut le type de port (Fa pour Fast Ethernet et Gi pour Gigabit Ethernet) et le numéro de port spécifique. **EXEMPLE :** Gi1/1 est un port Gigabit Ethernet 1.
Interface Counters (compteurs d'interface)	Ces compteurs vous permettent de voir l'état des octets reçus et envoyés et les paquets reçus et envoyés : • Octets In : nombre d'octets reçus par le port. • Octets Out : nombre d'octets envoyés par le port. • Ucast Packets In : nombre de paquets Ucast reçus par le port. • Ucast Packets Out : nombre de paquets Ucast envoyés par le port. • NUcast packets In : nombre de paquets de NUcast reçus par le port. • NUcast packets Out : nombre de paquets NUcast envoyés par le port. • Discards In : nombre de paquets entrants qui ont été rejetés. • Discards Out : nombre de paquets sortants qui ont été rejetés. • Errors In : nombre de paquets entrants contenant des erreurs. • Errors Out : nombre de paquets sortants contenant des erreurs. • Unknown Protos (Protocols) In : nombre de paquets entrants avec des protocoles inconnus.
Media Counters (compteurs de média)	Ces compteurs vous permettent de voir le nombre de collisions sur une liaison : • Single : nombre de collisions uniques. • Multiple : nombre de collisions multiples. • Late : nombre de collisions tardives. • Excessive : nombre de trames pour lesquelles la transmission échoue en raison de collisions excessives. • Ces compteurs vous permettent de visualiser des erreurs : • Alignment : nombre de trames reçues dont la longueur n'est pas un nombre entier d'octets. • FCS (Frame Check Sequence) : nombre de trames reçues qui ne passent pas la vérification FCS. • SQE Test Errors : nombre de fois où le message SQE TEST ERROR a été généré. • Deferred Transmissions : comptabilisation des transmissions différées par réseau occupé. • MAC Xmit Errors : nombre de trames en échec de transmission en raison d'une erreur interne de transmission de la sous-couche MAC. • MAC Recv Errors : nombre de trames en échec de réception en raison d'une erreur interne de réception de la sous-couche MAC. • Carrier Sense : nombre de fois où la condition de détection de la porteuse a été perdue ou n'a jamais été affirmée lors d'une tentative de transmission de trame. • Frame Too Long : nombre de trames reçues dépassant la taille maximum autorisée.

Diagnostics de câbles

La boîte de dialogue Cable Diagnostics fournit des informations permettant de diagnostiquer un problème de câble.

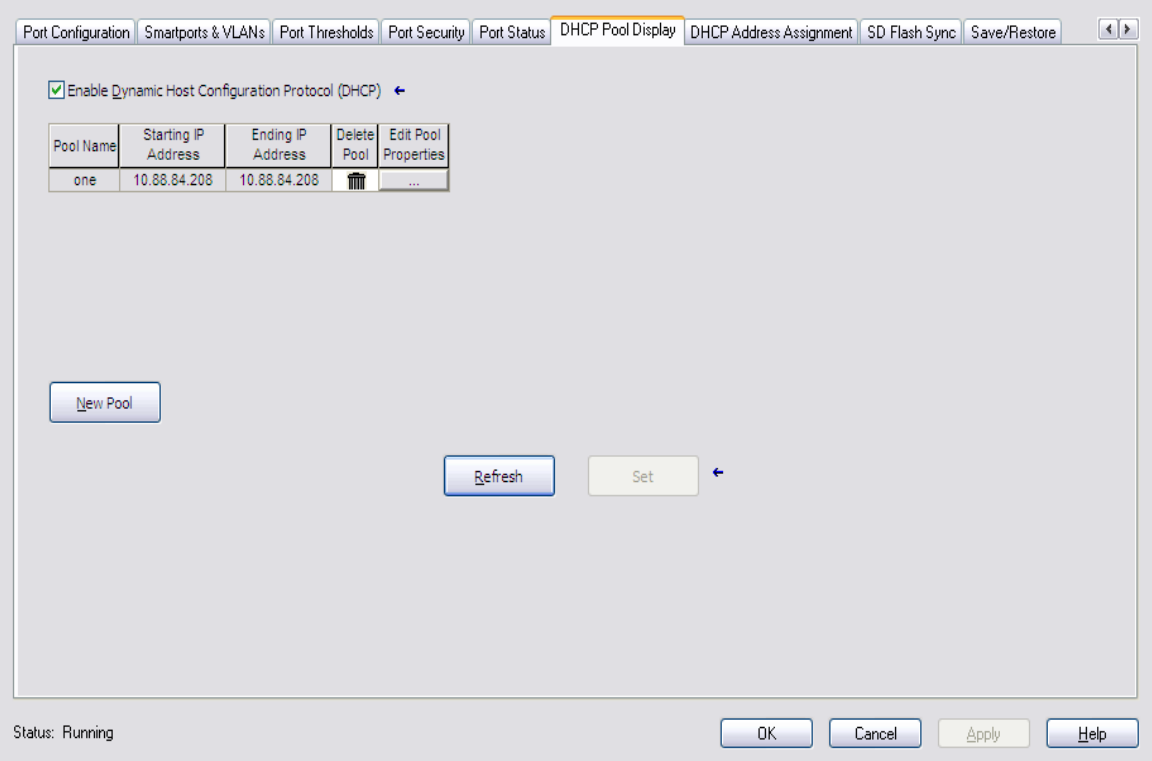
CONSEIL Les informations de cet onglet ne s'affichent pas si vous êtes hors ligne.

Tableau 37 - Champs de la boîte de dialogue Cable Diagnostics

Champ	Description
Port	Le port sélectionné pour la configuration. Le numéro de port inclut le type de port (Fa pour Fast Ethernet et Gi pour Gigabit Ethernet) et le numéro de port spécifique. **EXEMPLE :** Gi1/1 est un port Gigabit Ethernet 1.
Test last run on	Le moment de la dernière exécution de l'essai. Le format de date est mm/jj/aa hh:mm:ss tt. Si le test n'a jamais été exécuté, l'heure et toutes les informations de distance et d'état sont vides.
Pair	Chaque paire (paire de câbles en réseau) répertoriée individuellement. S'il n'existe pas de paire ou si le test n'a jamais été exécuté, cette zone est vide.
Status	Spécifie l'état de la liaison lors de la dernière exécution du test. S'il n'existe pas de paire ou si le test n'a jamais été exécuté, cette zone est vide. Pour la distance, si la paire est en état Normal, « No Break Detected » (pas de rupture détectée) s'affiche. Aucune distance ne s'affiche.
Distance to Break (distance à la rupture)	La distance jusqu'à la rupture à partir du switch pour chaque paire évaluée avec une valeur d'erreur positive ou négative, listée individuellement. Une valeur s'affiche uniquement lorsque l'état d'une paire existante n'est pas Normal. Cette zone est vide si le test n'a jamais exécuté auparavant. S'il n'existe pas de paire, « ??? » s'affiche.
Diagnose Cable	Cliquez pour lancer le test de diagnostic de câble (Diagnose Cable). Un avertissement d'interruption de connexion s'affiche : • Si vous êtes sûr de vouloir continuer le test, cliquez sur Yes (oui). Préparez-vous à entrer un mot de passe valable pour exécuter le test. • Si vous ne souhaitez pas exécuter le test, cliquez sur No (non) ou fermez la fenêtre. **IMPORTANT :** pour exécuter un test valable sur des ports gigabit, vous devez d'abord configurer le port gigabit comme un type RJ45 dans l'interface Internet de Device Manager, comme décrit dans Configuration des paramètres de port à la page 109. **IMPORTANT :** ce test peut interrompre les connexions vers le module et vers tous les autres modules connectés par l'intermédiaire de ce module. En outre, la connexion entre le poste de travail et l'automate peut être interrompue. Vous devez disposer des autorisations adéquates pour exécuter ce test.

Affichage du pool DHCP

Vous pouvez visualiser les informations de pool de l'adresse DHCP pour le switch à partir de l'onglet DHCP Pool Display. Vous pouvez visualiser de 0 à 15 pools. Ces informations sont recueillies directement à partir du switch. Chaque ligne représente une instance unique, et les valeurs d'instance ne peuvent pas être consécutives.



CONSEIL Les informations de cet onglet ne s'affichent pas si vous êtes hors ligne.

Tableau 38 - Champs de l'onglet DHCP Pool Display

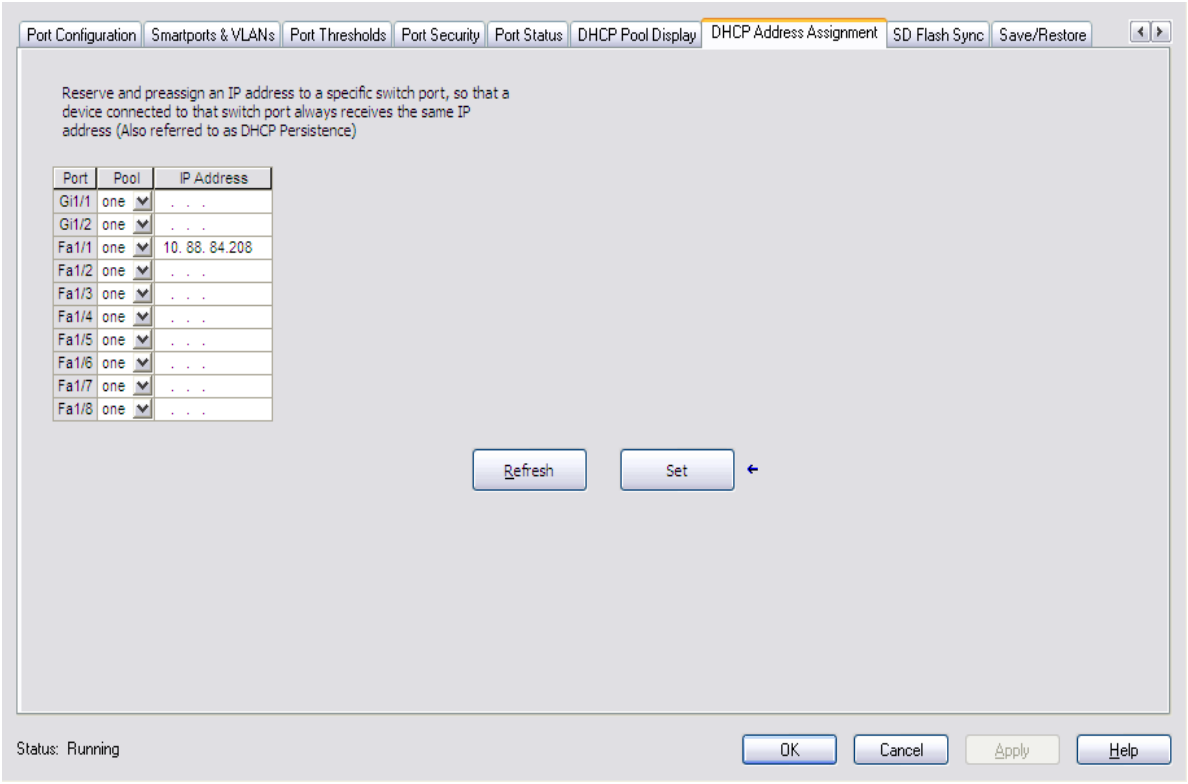
Champ	Description
Enable Dynamic Host Configuration Protocol (activer DHCP)	Permet d'activer ou de désactiver des pools. Si cette option est sélectionnée, toutes les commandes de la grille sont définies sur « en ligne » et les valeurs appropriées sont obtenues du switch et affichées. Si elle est désactivée, toutes les commandes de la grille sont définies sur « hors ligne ». À partir du clavier, appuyez sur Alt - D.
Pool Name	Affiche le nom du pool de l'adresse IP DHCP configuré sur le switch. Un pool d'adresse IP DHCP est une plage (ou pool) d'adresses IP disponibles que le switch peut affecter aux dispositifs connectés. Le nom peut comporter jusqu'à 31 caractères alphanumériques. Le nom ne peut pas contenir de ? ou de tabulation.
Starting IP Address (adresse IP de début)	Affiche l'adresse IP de début qui définit la plage d'adresses dans le pool d'adresses IP DHCP. Le format est une adresse numérique à 32-bits, écrite sous forme de quatre nombres séparés par des points (par exemple, 255.255.255.255). Chaque nombre peut être compris entre 0 et 255.
Ending IP Address (adresse IP de fin)	Affiche l'adresse IP de fin qui définit la plage d'adresses dans le pool d'adresses IP DHCP. Le format est une adresse numérique à 32 bits, écrite sous forme de quatre nombres séparés par des points (par exemple, 255.255.255.255). Chaque nombre peut être compris entre 0 et 255.
Delete Pool (effacement de pool)	Cliquez pour supprimer la ligne actuellement sélectionnée du pool DHCP. Ensuite, si vous cliquez sur Set, une boîte de dialogue de confirmation s'affiche et toutes les adresses résiduelles associées à la ligne sélectionnée du pool DHCP sont également supprimées. La fonction Delete Pool est disponible uniquement lorsque le switch est en ligne, que la case Enable Dynamic Host Configuration Protocol (DHCP) est cochée et que la ligne respective est renseignée. La fonction Delete Pool est grisée lorsque le switch est hors ligne et que la case Enable Dynamic Host Configuration Protocol (DHCP) est désactivée.
Refresh (actualisation)	Cliquez pour actualiser la commande de la grille avec les nouvelles données obtenues directement du switch. À partir du clavier, appuyez sur Alt-R. Si vous avez modifié une valeur dans la grille et cliqué sur Refresh avant de cliquer sur Set, toutes les valeurs dans la grille sont restaurées à leurs valeurs précédemment définies. La fonction Refresh est disponible uniquement lorsque le switch est en ligne. Le bouton Refresh est grisé lorsque le switch est hors ligne.

Tableau 38 - Champs de l'onglet DHCP Pool Display (suite)

Champ	Description
Edit Pool Properties (modifier les propriétés du pool)	Cliquez pour afficher la définition du Pool DHCP et la boîte de dialogue Edit (modifier), puis renseignez-la avec les valeurs provenant de l'instance correspondant à la ligne en cours. Le bouton Edit column est disponible uniquement lorsque le switch est en ligne, que la case Enable Dynamic Host Configuration Protocol (DHCP) est cochée et que la ligne respective est renseignée. Le bouton Edit column est grisé lorsque le switch est hors ligne et que la case Enable Dynamic Host Configuration Protocol (DHCP) est désactivée.
New Pool (nouveau pool)	Cliquez pour afficher la définition du Pool DHCP et la boîte de dialogue Edit (tous les champs sont vides et le bouton radio Custom n'est pas sélectionné). En outre, une nouvelle instance/ligne est ajoutée à la grille de la boîte de dialogue Module Properties - DHCP Pool Display. À partir du clavier, appuyez sur Alt - N. Le bouton New est disponible uniquement lorsque le switch est en ligne et que la case Enable Dynamic Host Configuration Protocol (DHCP) est cochée. Le bouton New est grisé lorsque le switch est hors ligne et que la case Enable Dynamic Host Configuration Protocol (DHCP) est décochée.
Set (établir)	Cliquez pour appliquer les modifications de l'attribut effectuées dans cette boîte de dialogue au switch. Seuls les attributs qui ont été modifiés sont appliqués au switch. La boîte de dialogue Enter Password (entrez le mot de passe) peut apparaître. Si une erreur se produit lors de la définition d'un attribut, l'opération Set est terminée et les valeurs d'attribut suivantes ne sont pas appliquées au switch. En outre, le bouton Set reste disponible. Le bouton Set est disponible uniquement lorsque le switch est en ligne et que l'une des valeurs d'attribut a changé. Le bouton Set est grisé lorsque le switch est hors ligne.

Attribution d'une adresse DHCP

Vous pouvez afficher et configurer la persistance DHCP à partir de l'onglet DHCP Address Assignment (attribution d'adresse DHCP). Avec la persistance DHCP, vous pouvez attribuer une adresse IP spécifique pour chaque port, afin que le dispositif connecté à un port spécifique reçoive la même adresse IP.



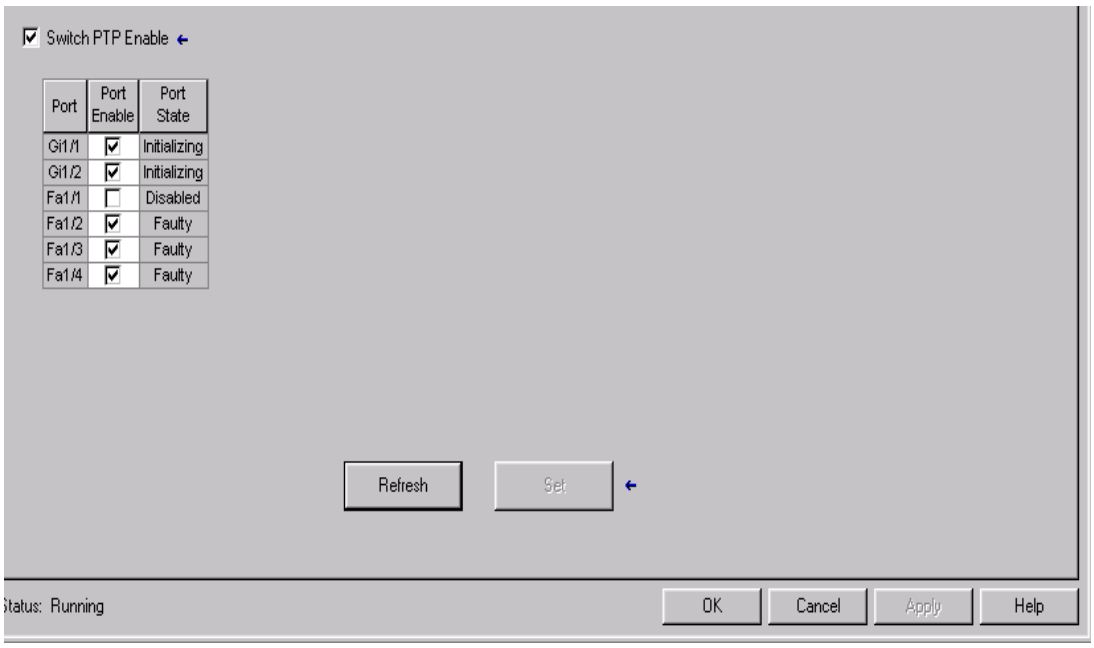
CONSEIL Les informations de cet onglet ne s'affichent pas si vous êtes hors ligne.

Tableau 39 - Champs de l'onglet DHCP Address Assignment

Champ	Description
Port	Affiche les ports disponibles pour la configuration. Le numéro de port inclut le type de port (Fa pour Fast Ethernet et Gi pour Gigabit Ethernet), le numéro du switch (1) et le numéro de port spécifique. **EXEMPLE :** • Gi1/1 est un port Gigabit Ethernet 1. • FA1/1 est un port Fast Ethernet 1.
Pool	Affiche les noms de pool depuis le pool d'adresses IP DHCP qui correspond aux instances disponibles dans le switch. Si vous supprimez toutes les lignes contenant des pools dans l'onglet DHCP Pool Display de la boîte de dialogue Module Properties (propriétés du module) et que vous cliquez sur Refresh, le champ Pool est vide. Le champ Pool est disponible lorsque le switch est en ligne et apparaît en grisé lorsqu'il est hors ligne.
IP Address (adresse IP)	Affiche l'adresse IP affectée au port du switch. Le format est une adresse numérique à 32 bits, écrite sous forme de quatre nombres séparés par des points (par exemple, 255.255.255.255). Chaque nombre peut être compris entre 0 et 255. L'adresse IP est disponible uniquement lorsque le switch est en ligne et grisée lorsqu'il est hors ligne.
Refresh (actualisation)	Cliquez pour actualiser la commande de la grille avec les nouvelles données obtenues directement du switch. À partir du clavier, appuyez sur Alt-R. Si vous avez modifié une valeur dans la grille et cliqué sur Refresh avant de cliquer sur Set, toutes les valeurs dans la grille sont restaurées à leurs valeurs précédemment définies. Le bouton Refresh est disponible uniquement lorsque le switch est en ligne. Le bouton Refresh est grisé lorsque le switch est hors ligne.
Set (établir)	Cliquez pour appliquer les modifications effectuées sur le switch dans cette boîte de dialogue. La boîte de dialogue Enter Password (entrez le mot de passe) peut apparaître.

Configuration de Time Sync

Utilisez cette fonctionnalité pour synchroniser les ports via PTP. PTP synchronise à la nanoseconde près les horloges en temps réel des dispositifs d'un réseau. À l'aide de la sélection de l'horloge maître, le switch identifie le port connecté à un dispositif avec la meilleure source d'horloge. Le switch synchronise alors son horloge interne avec la meilleure source d'horloge et le port du switch est défini sur l'état maître. La source d'horloge la plus précise dans le réseau est dénommée l'horloge grand-maître. Pour plus d'informations à propos de cette fonctionnalité, voir Synchronisation du temps CIP Sync (protocole PTP) à la page 80.



CONSEIL Les informations de cet onglet ne s'affichent pas si vous êtes hors ligne.

Tableau 40 - Champs de l'onglet Time Sync Configuration

Champ	Description
Switch PTP Enable (validation du PTP du switch)	Cochez pour activer le PTP sur le dispositif. Par défaut, PTP est activé sur tous les ports Fast Ethernet et Gigabit Ethernet du switch. Décochez pour désactiver le PTP sur le dispositif. Les fonctions Port Enable et Port State apparaissent en grisé lorsque la case Switch PTP Enable est décochée.
Port	Affiche le port sélectionné pour la configuration. Le numéro de port inclut le type de port (Fa pour Fast Ethernet et Gi pour Gigabit Ethernet) et le numéro de port spécifique. **EXEMPLE :** Gi1/1 est un port Gigabit Ethernet 1.
Port Enable (activation du port)	Cochez pour activer la configuration du port sur le dispositif. Décochez pour désactiver la configuration du port sur le dispositif. La fonction Port Enable apparaît en grisé lorsque la case Switch PTP Enable est désactivée.
Port State (état du port)	Affiche l'état actuel du port PTP sur le dispositif. Valeurs valables : • Initializing (initialisation en cours) • Faulty (en défaut) • Disabled (désactivé) • Listening (en écoute) • Pre-Master (pré maître) • Master (maître) • Uncalibrated (non étalonné) • Slave (esclave) Le champ Port State est vide et grisé lorsque la case Switch PTP Enable est décochée.
Refresh (actualisation)	Cliquez pour actualiser l'onglet avec les nouvelles données provenant du switch.
Set (établir)	Cliquez pour envoyer les réglages au switch. La boîte de dialogue Enter Password (entrez le mot de passe) peut apparaître. Préparez-vous à entrer un mot de passe valide pour établir les réglages de configuration. Le bouton Set est grisé lorsque le switch est hors ligne.

Configuration de NAT

Vous pouvez créer des instances NAT à partir de l'onglet NAT.

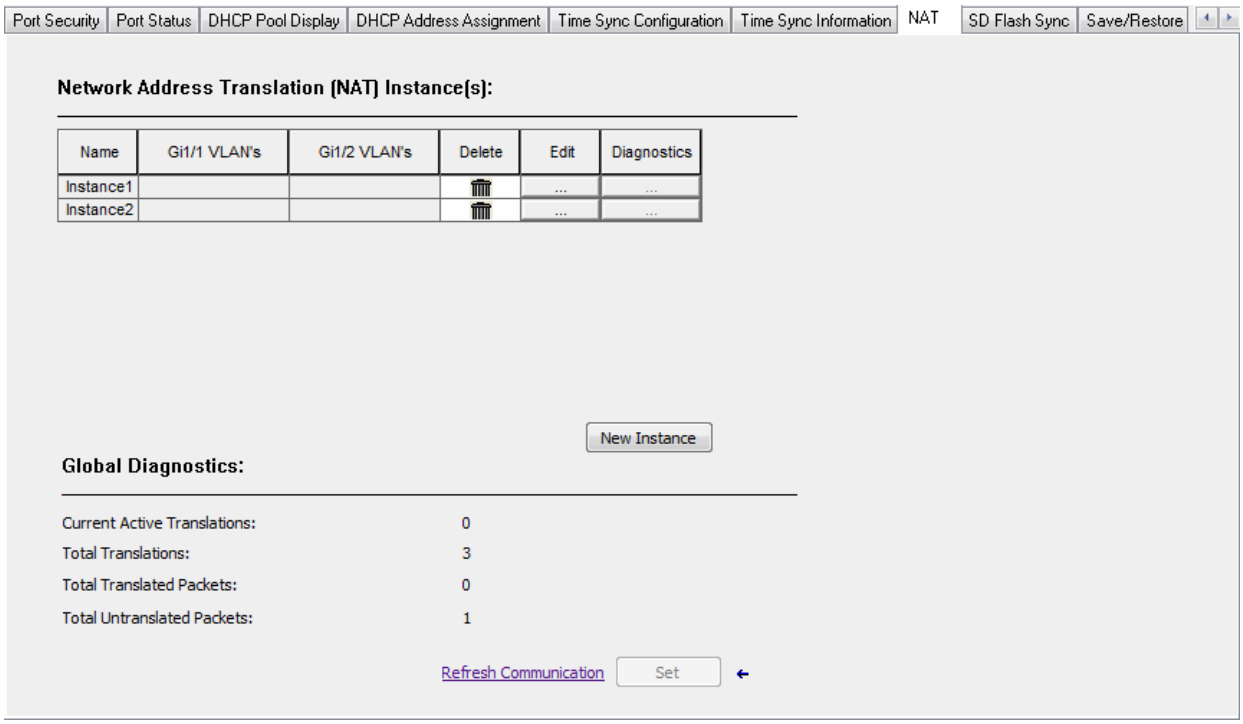


Tableau 41 - Champs de l'onglet NAT

Champ	Description
Name (nom)	Affiche le nom unique de l'instance NAT.
Gi1/1 VLANs	Affiche les VLAN assignés à chaque instance NAT sur le port Gi1/1.
Gi1/2 VLANs	Affiche les VLAN assignés à chaque instance NAT sur le port Gi1/2.
Delete (supprimer)	Cliquez pour supprimer définitivement une instance NAT. Le switch supprime l'instance lorsque vous cliquez sur Set.
Edit (modifier)	Cliquez pour modifier la configuration d'une instance NAT.
Diagnostics	Cliquez pour afficher les diagnostics de traduction d'une instance. Voir page 200.
New Instance (nouvelle instance)	Cliquez pour créer une instance NAT. Voir page 188.
Current Active Translations (traductions actives actuelles)	Affiche le nombre total de traductions survenues dans les 90 dernières secondes sur toutes les instances NAT.
Total Translations (traductions totales)	Affiche le nombre total de traductions sur toutes les instances NAT.
Total Translated Packets (paquets traduits totaux)	Affiche le nombre total de paquets traduits sur toutes les instances NAT.
Total Untranslated Packets (paquets non traduits totaux)	Affiche le nombre total de paquets qui ont été contournés sur toutes les instances NAT.
Refresh Communication (actualiser la communication)	Cliquez pour actualiser toutes les données de l'onglet.
Set (établir)	Cliquez pour supprimer une instance NAT sur le switch après avoir cliqué sur l'icône de corbeille à côté de l'instance.

Pour configurer NAT, suivez l'une des procédures ci-dessous, en fonction de votre application :

- Création des instances NAT pour le trafic routé via un switch de couche 3 ou un routeur

  Pour un exemple de cette application, consultez Figure 4 à la page 82.
- Création des instances NAT pour le trafic routé via un switch de Couche 2

  Pour un exemple de cette application, consultez Figure 5 à la page 82.

IMPORTANT Mettez en place tous les rôles Smartport et VLAN avant de créer des instances NAT.

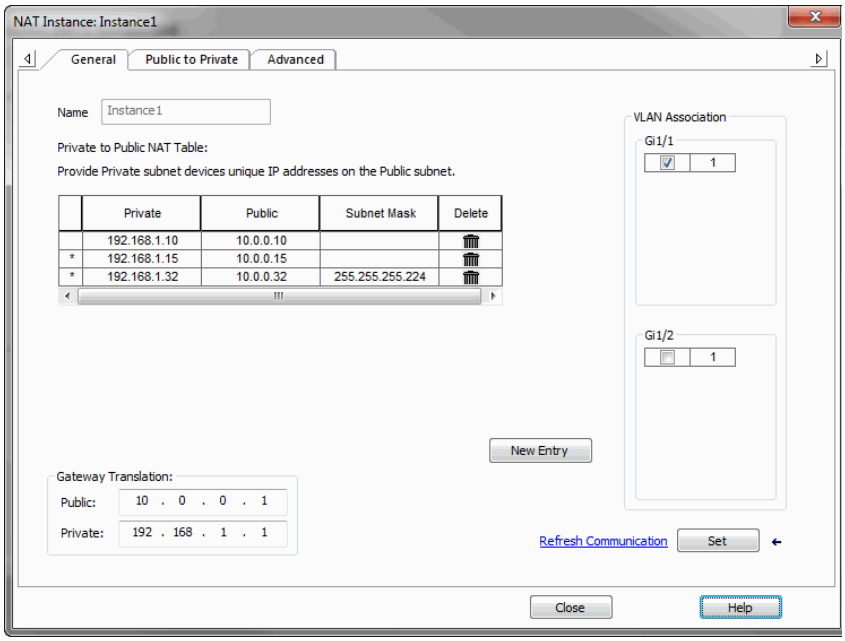
Si vous modifiez un rôle Smartport ou le VLAN natif pour un port associé à une instance NAT, vous devez réaffecter les VLAN à l'instance NAT.

IMPORTANT À la suite d'un transfert de couche 2, les sessions de trafic en cours restent maintenues jusqu'à la déconnexion manuelle. Si vous modifiez une traduction existante, vous devez déconnecter manuellement les sessions de trafic associées à toutes les séances pour que la nouvelle traduction puisse être effective.

Création des instances NAT pour le trafic routé via un switch de couche 3 ou un routeur

Pour créer une instance NAT pour le trafic routé via un switch de couche 3 ou un routeur, suivez les étapes ci-après.

1. À partir de l'onglet NAT, cliquez sur New Instance (nouvelle instance) pour afficher l'onglet General de la boîte de dialogue NAT Instance .



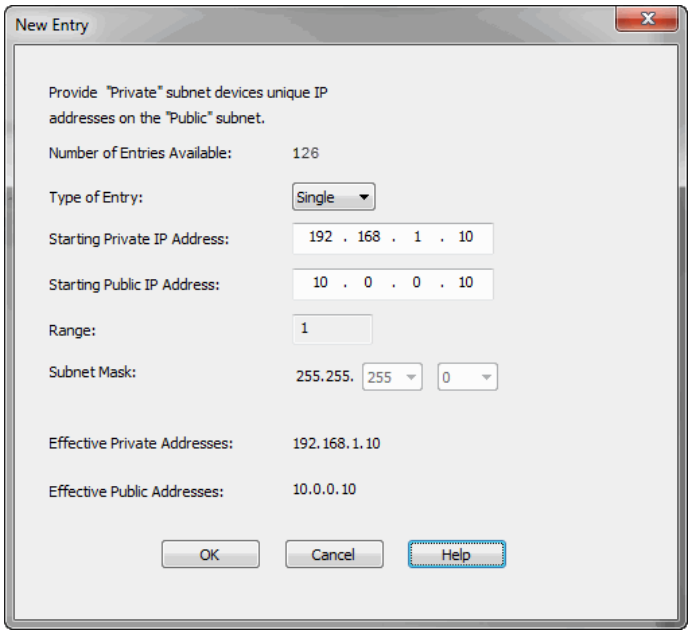
2. Dans le champ Name (nom), tapez un nom unique pour identifier l'instance.

   Le nom de l'instance ne peut pas inclure d'espaces ni dépasser 32 caractères.

3. Dans la zone VLAN Association, cochez la case en regard de chaque VLAN à affecter à l'instance.

   Pour plus d'informations sur les affectations VLAN, voir page 83.

4. Cliquez sur New Entry (nouvelle saisie) pour afficher la boîte de dialogue correspondante.



5. Effectuez l'une des procédures suivantes :

   - Pour traduire une seule adresse pour un dispositif sur le sous-réseau privé qui a besoin de communiquer sur le sous-réseau public, remplissez les champs ci-dessous.

Champ	Description
Type of Entry (type de saisie)	Choisissez Single. Il s'agit de la valeur par défaut.
Starting Private IP Address (adressse IP privée de début)	Tapez l'adresse existante pour le dispositif sur le sous-réseau privé.
Starting Public IP Address (adressse IP publique de début)	Tapez une adresse publique unique pour représenter le dispositif.
Effective Private Addresses (adresses privées effectives)	Affiche l'adresse existante pour le dispositif sur le sous-réseau privé qui est configuré pour la traduction. Si la zone est vide, vérifiez que les valeurs des champs ci-dessus sont valides.
Effective Public Addresses (adresses publiques effectives)	Affiche l'adresse publique unique représentant le dispositif. Si la zone est vide, vérifiez que les valeurs des champs ci-dessus sont valides.

   - Pour traduire une plage d'adresses pour des dispositifs du sous-réseau privé qui a besoin de communiquer sur le sous-réseau public, remplissez les champs ci-dessous.

Champ	Description
Type of Entry (type de saisie)	Choisissez Range (plage).
Starting Private IP Address (adressse IP privée de début)	Tapez l'adresse existante de début pour le dispositif sur le sous-réseau privé.
Starting Public IP Address (adressse IP publique de début)	Tapez une adresse publique unique de début pour représenter le dispositif.

Champ	Description
Range (plage)	Tapez le nombre d'adresses à inclure dans la plage. Valeurs valables : 1 à 128 Valeur par défaut = 1 **IMPORTANT :** chaque adresse dans la plage compte comme une saisie de traduction. Le switch prend en charge un maximum de 128 saisies de traduction.
Effective Private Addresses (adresses privées effectives)	Affiche la plage des adresses existantes pour les dispositifs sur le sous-réseau privé qui sont configurés pour la traduction. Si la zone est vide, vérifiez que les valeurs des champs ci-dessus sont valides.
Effective Public Addresses (adresses publiques effectives)	Affiche la plage d'adresses publiques uniques pour représenter les dispositifs. Si la zone est vide, vérifiez que les valeurs des champs ci-dessus sont valides.

- Pour traduire toutes les adresses dans le sous-réseau privé ou une partie du sous-réseau privé, remplissez les champs ci-dessous.

Champ	Description	
Type of Entry (type de saisie)	Choisissez Subnet (sous-réseau).	
Starting Private IP Address (adressse IP privée de début)	Tapez l'adresse existante de début pour un dispositif sur le sous-réseau privé. Cette adresse doit correspondre à la taille du masque de sous-réseau à traduire comme illustré ci-dessous.	
	Masque de sous-réseau	**Adresse sous-réseau privé de début**
	255.255.0.0	Les deux derniers octets doivent se terminer par 0. **EXEMPLE :** 192.168.0.0
	255.255.255.0	Le dernier octet doit se terminer par 0. **EXEMPLE :** 192.168.1.0
	255.255.255.128	Le dernier octet doit se terminer par 0 ou 128. **EXEMPLE :** 192.168.1.0 ou 192.168.1.128
	255.255.255.192	Le dernier octet doit se terminer par l'un des nombres suivants : 0, 64, 128, 192. **EXEMPLE :** 192.168.1.64
	255.255.255.224	Le dernier octet doit se terminer par l'un des nombres suivants : 0, 32, 64, 96, 128, 160, 192, 224. **EXEMPLE :** 192.168.1.32
	255.255.255.240	Le dernier octet doit se terminer par l'un des nombres suivants : 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240. **EXEMPLE :** 192.168.1.16

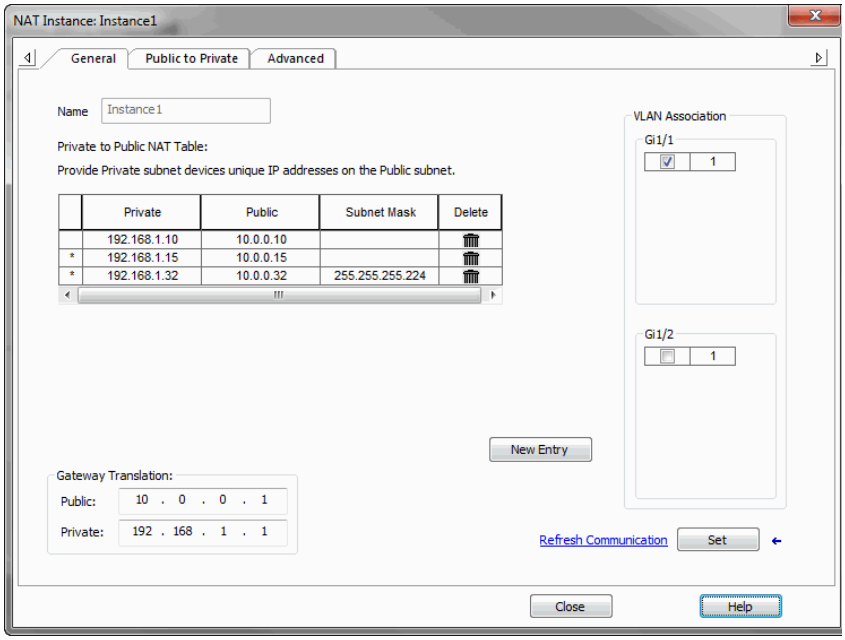
<table>
<tr><th>Champ</th><th colspan="2">Description</th></tr>
<tr><td>Starting Public IP Address (adressse IP publique de début)</td><td colspan="2">Tapez une adresse publique unique de début pour représenter les dispositifs. Cette adresse doit correspondre à la taille du masque de sous-réseau à traduire comme illustré ci-dessous.</td></tr>
<tr><td></td><td>Masque de sous-réseau</td><td>Adresse sous-réseau public de début</td></tr>
<tr><td></td><td>255.255.0.0</td><td>Les deux derniers octets doivent se terminer par 0.
EXEMPLE : 10.200.0.0</td></tr>
<tr><td></td><td>255.255.255.0</td><td>Le dernier octet doit se terminer par 0.
EXEMPLE : 10.200.1.0</td></tr>
<tr><td></td><td>255.255.255.128</td><td>Le dernier octet doit se terminer par 0 ou 128.
EXEMPLE : 10.200.1.0 ou 10.200.1.128</td></tr>
<tr><td></td><td>255.255.255.192</td><td>Le dernier octet doit se terminer par l'un des nombres suivants : 0, 64, 128, 192.
EXEMPLE : 10.200.1.64</td></tr>
<tr><td></td><td>255.255.255.224</td><td>Le dernier octet doit se terminer par l'un des nombres suivants : 0, 32, 64, 96, 128, 160, 192, 224.
EXEMPLE : 10.200.1.32</td></tr>
<tr><td></td><td>255.255.255.240</td><td>Le dernier octet doit se terminer par l'un des nombres suivants : 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240.
EXEMPLE : 10.200.1.16</td></tr>
<tr><td>Masque de sous-réseau</td><td colspan="2">À partir des menus déroulants, choisissez le masque de sous-réseau pour les adresses à traduire.
Valeurs valables :
• Classe B : 255.255.0.0
• Classe C : 255.255.255.0
• Portion de Classe C :
– 255.255.255.128 (fournit 128 adresses par entrée de traduction)
– 255.255.255.192 (fournit 64 adresses par entrée de traduction)
– 255.255.255.224 (fournit 32 adresses par entrée de traduction)
– 255.255.255.240 (fournit 16 adresses par entrée de traduction)</td></tr>
<tr><td>Effective Private Addresses (adresses privées effectives)</td><td colspan="2">Affiche la plage des adresses existantes pour les dispositifs sur le sous-réseau privé qui sont configurés pour la traduction.
Si la zone est vide, vérifiez que les valeurs des champs ci-dessus sont valides.</td></tr>
<tr><td>Effective Public Addresses (adresses publiques effectives)</td><td colspan="2">Affiche la plage d'adresses publiques uniques pour représenter les dispositifs.
Si la zone est vide, vérifiez que les valeurs des champs ci-dessus sont valides.</td></tr>
</table>

6. Cliquez sur OK.
7. Complétez les champs Gateway Translation (traduction de passerelle) pour permettre aux dispositifs sur le sous-réseau public de communiquer avec les dispositifs sur le sous-réseau privé :
   - Public - Tapez l'adresse par défaut de la passerelle du switch de Couche 3 ou du routeur connecté au port de liaison montante du switch.
   - Privé - Tapez une adresse IP unique pour représenter le switch de Couche 3 ou le routeur sur le réseau privé.
8. Pour configurer les autorisations de trafic et les corrections des paquets, veuillez procéder selon Configuration des autorisations et des corrections de trafic à la page 198.
9. Cliquez sur Set (régler).

Création des instances NAT pour le trafic routé via un switch de Couche 2

Pour créer une instance NAT pour le trafic routé via un switch de Couche 2, suivez ces étapes.

1. À partir de l'onglet NAT, cliquez sur New Instance (nouvelle instance) pour afficher la boîte de dialogue NAT Instance (instance NAT).



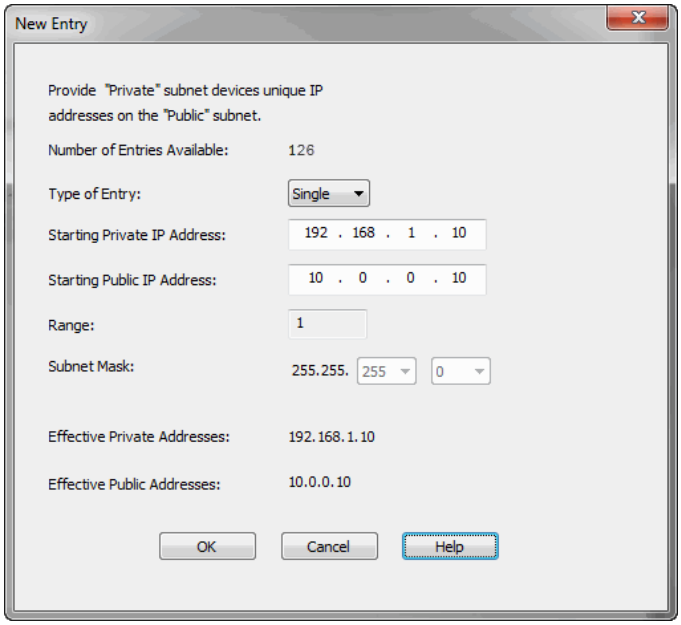
2. Dans le champ Name (nom), tapez un nom unique pour identifier l'instance.

   Le nom de l'instance ne peut pas inclure d'espaces ni dépasser 32 caractères.

3. À partir de la liste des VLAN sur la droite, cochez la case en regard de chaque VLAN à affecter à l'instance.

   Pour plus d'informations sur les affectations VLAN, voir page 83.

4. Cliquez sur New Entry (nouvelle saisie) pour afficher la boîte de dialogue correspondante.



5. Effectuez l'une des procédures suivantes :

- Pour traduire une seule adresse pour un dispositif sur le sous-réseau privé qui a besoin de communiquer sur le sous-réseau public, remplissez les champs ci-dessous.

Champ	Description
Type of Entry (type de saisie)	Choisissez Single. Il s'agit de la valeur par défaut.
Starting Private IP Address (adressse IP privée de début)	Tapez l'adresse existante pour le dispositif sur le sous-réseau privé.
Starting Public IP Address (adressse IP publique de début)	Tapez une adresse publique unique pour représenter le dispositif.
Effective Private Addresses (adresses privées effectives)	Affiche l'adresse existante pour le dispositif sur le sous-réseau privé qui est configuré pour la traduction. Si la zone est vide, vérifiez que les valeurs des champs ci-dessus sont valides.
Effective Public Addresses (adresses publiques effectives)	Affiche l'adresse publique unique représentant le dispositif. Si la zone est vide, vérifiez que les valeurs des champs ci-dessus sont valides.

- Pour traduire une plage d'adresses pour des dispositifs du sous-réseau privé qui a besoin de communiquer sur le sous-réseau public, remplissez les champs ci-dessous.

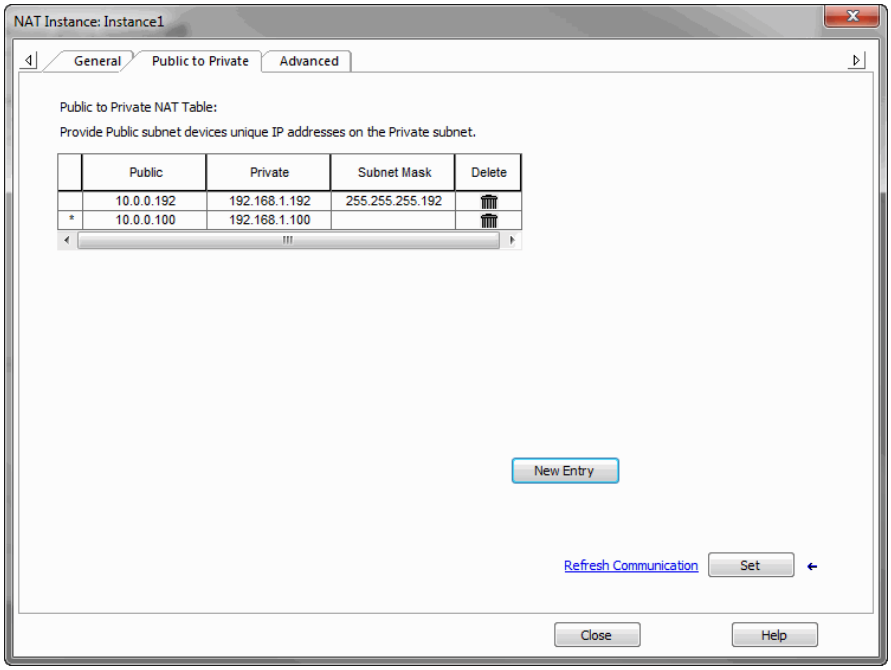
Champ	Description
Type of Entry (type de saisie)	Choisissez Range (plage).
Starting Private IP Address (adressse IP privée de début)	Tapez l'adresse existante de début pour le dispositif sur le sous-réseau privé.
Starting Public IP Address (adressse IP publique de début)	Tapez une adresse publique unique de début pour représenter les dispositifs.
Range (plage)	Tapez le nombre d'adresses à inclure dans la plage. Valeurs valables : 1 à 128 Valeur par défaut = 1 **IMPORTANT :** chaque adresse dans la plage compte comme une saisie de traduction. Le switch prend en charge un maximum de 128 saisies de traduction.
Effective Private Addresses (adresses privées effectives)	Affiche la plage des adresses existantes pour les dispositifs sur le sous-réseau privé qui sont configurés pour la traduction. Si la zone est vide, vérifiez que les valeurs des champs ci-dessus sont valides.
Effective Public Addresses (adresses publiques effectives)	Affiche la plage d'adresses publiques uniques pour représenter les dispositifs. Si la zone est vide, vérifiez que les valeurs des champs ci-dessus sont valides.

- Pour traduire toutes les adresses dans le sous-réseau privé ou une partie du sous-réseau privé, remplissez les champs ci-dessous.

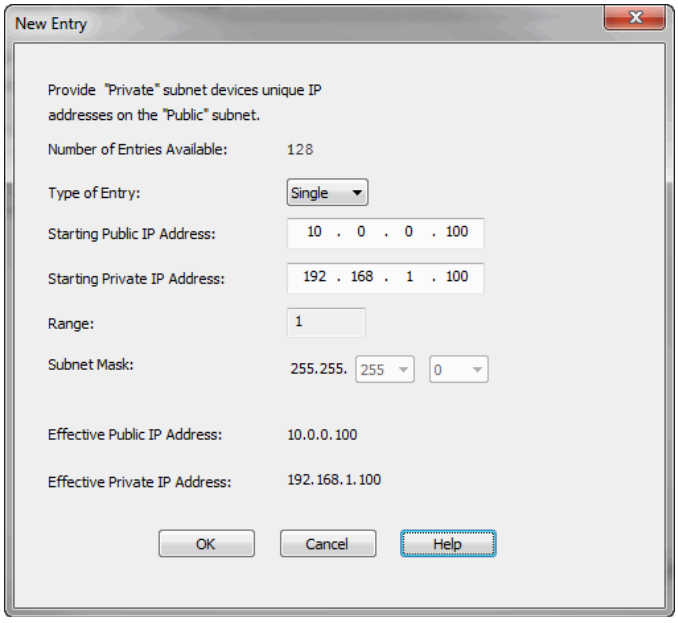
Champ	Description	
Type of Entry (type de saisie)	Choisissez Subnet (sous-réseau).	
Starting Private IP Address (adressse IP privée de début)	Tapez l'adresse existante de début pour un dispositif sur le sous-réseau privé. Cette adresse doit correspondre à la taille du masque de sous-réseau à traduire comme illustré ci-dessous.	
	Masque de sous-réseau	**Adresse sous-réseau privé de début**
	255.255.0.0	Les deux derniers octets doivent se terminer par 0. **EXEMPLE :** 192.168.0.0
	255.255.255.0	Le dernier octet doit se terminer par 0. **EXEMPLE :** 192.168.1.0
	255.255.255.128	Le dernier octet doit se terminer par 0 ou 128. **EXEMPLE :** 192.168.1.0 ou 192.168.1.128
	255.255.255.192	Le dernier octet doit se terminer par l'un des nombres suivants : 0, 64, 128, 192. **EXEMPLE :** 192.168.1.64
	255.255.255.224	Le dernier octet doit se terminer par l'un des nombres suivants : 0, 32, 64, 96, 128, 160, 192, 224. **EXEMPLE :** 192.168.1.32
	255.255.255.240	Le dernier octet doit se terminer par l'un des nombres suivants : 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240. **EXEMPLE :** 192.168.1.16
Starting Public IP Address (adressse IP publique de début)	Tapez une adresse publique unique de début pour représenter les dispositifs. Cette adresse doit correspondre à la taille du masque de sous-réseau à traduire comme illustré ci-dessous.	
	Masque de sous-réseau	**Adresse sous-réseau public de début**
	255.255.0.0	Les deux derniers octets doivent se terminer par 0. **EXEMPLE :** 10.200.0.0
	255.255.255.0	Le dernier octet doit se terminer par 0. **EXEMPLE :** 10.200.1.0
	255.255.255.128	Le dernier octet doit se terminer par 0 ou 128. **EXEMPLE :** 10.200.1.0 ou 10.200.1.128
	255.255.255.192	Le dernier octet doit se terminer par l'un des nombres suivants : 0, 64, 128, 192. **EXEMPLE :** 10.200.1.64
	255.255.255.224	Le dernier octet doit se terminer par l'un des nombres suivants : 0, 32, 64, 96, 128, 160, 192, 224. **EXEMPLE :** 10.200.1.32
	255.255.255.240	Le dernier octet doit se terminer par l'un des nombres suivants : 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240. **EXEMPLE :** 10.200.1.16
Subnet Mask (masque de sous-réseau)	À partir des menus déroulants, choisissez le masque de sous-réseau pour les adresses à traduire. Valeurs valables : • Classe B : 255.255.0.0 • Classe C : 255.255.255.0 • Portion de Classe C : – 255.255.255.128 (fournit 128 adresses par entrée de traduction) – 255.255.255.192 (fournit 64 adresses par entrée de traduction) – 255.255.255.224 (fournit 32 adresses par entrée de traduction) – 255.255.255.240 (fournit 16 adresses par entrée de traduction)	

Champ	Description
Effective Private Addresses (adresses privées effectives)	Affiche la plage des adresses existantes pour les dispositifs sur le sous-réseau privé qui sont configurés pour la traduction. Si la zone est vide, vérifiez que les valeurs des champs ci-dessus sont valides.
Effective Public Addresses (adresses publiques effectives)	Affiche la plage d'adresses publiques uniques pour représenter les dispositifs. Si la zone est vide, vérifiez que les valeurs des champs ci-dessus sont valides.

6. Cliquez sur OK.
7. Cliquez sur l'onglet Public to Private (privé vers publique).



8. Cliquez sur New Entry (nouvelle saisie) pour afficher la boîte de dialogue correspondante.



9. Effectuez l'une des procédures suivantes :

- Pour traduire une seule adresse pour un dispositif sur le sous-réseau public qui a besoin de communiquer sur le sous-réseau privé, remplissez les champs ci-dessous.

Champ	Description
Type of Entry (type de saisie)	Choisissez Single. Il s'agit de la valeur par défaut.
Starting Public IP Address (adressse IP publique de début)	Tapez l'adresse existante pour le dispositif sur le sous-réseau public.
Starting Private IP Address (adressse IP privée de début)	Tapez une adresse privée unique pour représenter le dispositif.
Effective Public Addresses (adresses publiques effectives)	Affiche l'adresse existante pour le dispositif sur le sous-réseau public qui est configuré pour la traduction. Si la zone est vide, vérifiez que les valeurs des champs ci-dessus sont valides.
Effective Private Addresses (adresses privées effectives)	Affiche l'adresse privée unique représentant le dispositif. Si la zone est vide, vérifiez que les valeurs des champs ci-dessus sont valides.

- Pour traduire une plage d'adresses pour des dispositifs du sous-réseau public qui a besoin de communiquer sur le sous-réseau privé, remplissez les champs ci-dessous.

Champ	Description
Type of Entry (type de saisie)	Choisissez Range (plage).
Starting Public IP Address (adressse IP publique de début)	Tapez l'adresse de début existante pour le dispositif sur le sous-réseau public.
Starting Private IP Address (adressse IP privée de début)	Tapez une adresse de début privée unique pour représenter les dispositifs.
Range (plage)	Tapez le nombre d'adresses à inclure dans la plage. Valeurs valables : 1 à 128 Valeur par défaut = 1 **IMPORTANT :** chaque adresse dans la plage compte comme une saisie de traduction. Le switch prend en charge un maximum de 128 saisies de traduction.
Effective Public Addresses (adresses publiques effectives)	Affiche la plage des adresses existantes pour les dispositifs sur le sous-réseau public qui sont configurés pour la traduction. Si la zone est vide, vérifiez que les valeurs des champs ci-dessus sont valides.
Effective Private Addresses (adresses privées effectives)	Affiche la plage d'adresses privées uniques pour représenter les dispositifs. Si la zone est vide, vérifiez que les valeurs des champs ci-dessus sont valides.

- Pour traduire toutes les adresses dans le sous-réseau public ou une partie du sous-réseau public, renseignez les champs comme décrit dans le tableau ci-dessous.

Champ	Description	
Type of Entry (type de saisie)	Choisissez Subnet (sous-réseau).	
Starting Public IP Address (adressse IP publique de début)	Tapez l'adresse de début existante pour le dispositif sur le sous-réseau public. Cette adresse doit correspondre à la taille du masque de sous-réseau à traduire comme illustré ci-dessous.	
	Masque de sous-réseau	**Adresse sous-réseau public de début**
	255.255.0.0	Les deux derniers octets doivent se terminer par 0. **EXEMPLE :** 10.200.0.0
	255.255.255.0	Le dernier octet doit se terminer par 0. **EXEMPLE :** 10.200.1.0
	255.255.255.128	Le dernier octet doit se terminer par 0 ou 128. **EXEMPLE :** 10.200.1.0 ou 10.200.1.128
	255.255.255.192	Le dernier octet doit se terminer par l'un des nombres suivants : 0, 64, 128, 192. **EXEMPLE :** 10.200.1.64
	255.255.255.224	Le dernier octet doit se terminer par l'un des nombres suivants : 0, 32, 64, 96, 128, 160, 192, 224. **EXEMPLE :** 10.200.1.32
	255.255.255.240	Le dernier octet doit se terminer par l'un des nombres suivants : 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240. **EXEMPLE :** 10.200.1.16
Starting Private IP Address (adressse IP privée de début)	Tapez une adresse de début privée unique pour représenter les dispositifs. Cette adresse doit correspondre à la taille du masque de sous-réseau à traduire comme illustré ci-dessous.	
	Masque de sous-réseau	**Adresse sous-réseau privé de début**
	255.255.0.0	Les deux derniers octets doivent se terminer par 0. **EXEMPLE :** 192.168.0.0
	255.255.255.0	Le dernier octet doit se terminer par 0. **EXEMPLE :** 192.168.1.0
	255.255.255.128	Le dernier octet doit se terminer par 0 ou 128. **EXEMPLE :** 192.168.1.0 ou 192.168.1.128
	255.255.255.192	Le dernier octet doit se terminer par l'un des nombres suivants : 0, 64, 128, 192. **EXEMPLE :** 192.168.1.64
	255.255.255.224	Le dernier octet doit se terminer par l'un des nombres suivants : 0, 32, 64, 96, 128, 160, 192, 224. **EXEMPLE :** 192.168.1.32
	255.255.255.240	Le dernier octet doit se terminer par l'un des nombres suivants : 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240. **EXEMPLE :** 192.168.1.16

Champ	Description
Masque de sous-réseau	À partir des menus déroulants, choisissez le masque de sous-réseau pour les adresses à traduire. Valeurs valables : • Classe B : 255.255.0.0 • Classe C : 255.255.255.0 • Portion de Classe C : – 255.255.255.128 (fournit 128 adresses par entrée de traduction) – 255.255.255.192 (fournit 64 adresses par entrée de traduction) – 255.255.255.224 (fournit 32 adresses par entrée de traduction) – 255.255.255.240 (fournit 16 adresses par entrée de traduction)
Effective Public Addresses (adresses publiques effectives)	Affiche la plage des adresses existantes pour les dispositifs sur le sous-réseau public qui sont configurés pour la traduction. Si la zone est vide, vérifiez que les valeurs des champs ci-dessus sont valides.
Effective Private Addresses (adresses privées effectives)	Affiche la plage d'adresses privées uniques pour représenter les dispositifs. Si la zone est vide, vérifiez que les valeurs des champs ci-dessus sont valides.

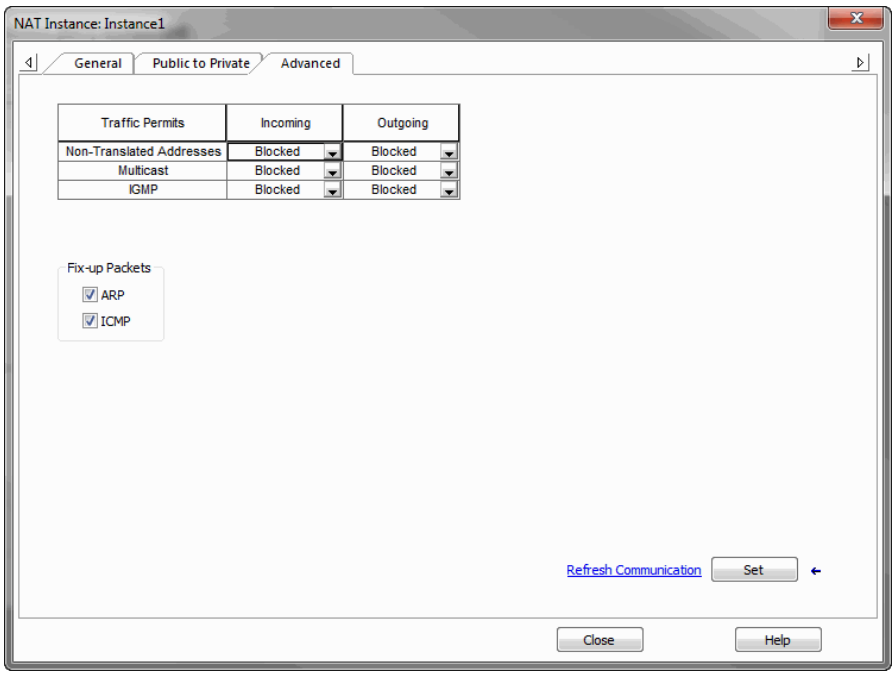
10. Cliquez sur OK.
11. (facultatif). Pour configurer les autorisations de trafic et les corrections des paquets, veuillez procéder selon Configuration des autorisations et des corrections de trafic à la page 198.
12. Cliquez sur Set (définir).

Configuration des autorisations et des corrections de trafic

Soyez prudent lors de la configuration des autorisations et des corrections de trafic. Nous vous recommandons d'utiliser les valeurs par défaut.

Pour configurer les autorisations et les corrections de paquets, procédez comme suit.

1. Cliquez sur l'onglet Advanced (avancé).



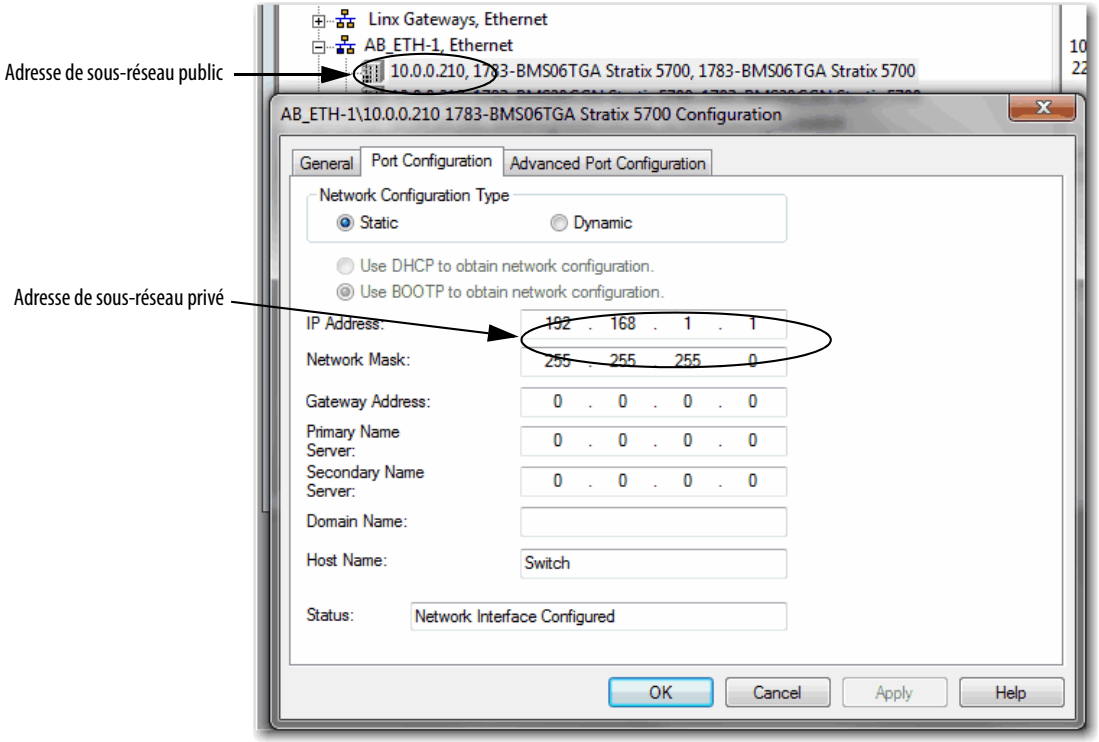
2. Dans la grille Traffic Permits, choisissez l'une des options suivantes pour les paquets entrants et sortants qui ne sont pas gérés par NAT :
   - Pass-Through - autorise les paquets à passer la frontière NAT.
   - Blocked - les paquets sont abandonnés.
3. Dans la zone Fix-up Packets, cochez ou décochez les cases permettant d'activer ou désactiver les corrections de protocole pour ARP et ICMP.

   Par défaut, les corrections sont activées à la fois pour ARP et ICMP.

Visualisation des traductions d'adresse dans le logiciel RSLinx

Le driver Ethernet du logiciel RSLinx prend en charge les dispositifs dotés de traductions d'adresse. Si l'adresse du dispositif est configurée pour la traduction, son adresse de sous-réseau public apparaît dans la boîte de dialogue principale du logiciel RSLinx. Cependant, son adresse de sous-réseau privé s'affiche dans les propriétés de configuration du dispositif.

Figure 9 - Adresses de sous-réseau public et privé dans le logiciel RSLinx

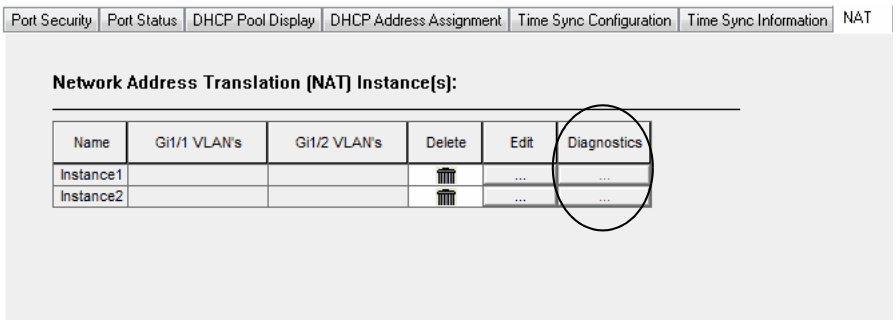


Diagnostics NAT

Pour chaque instance NAT, vous pouvez surveiller les diagnostics suivants :

- Diagnostics à la fois pour les traductions privées et publiques
- Diagnostics pour les traductions privées uniquement
- Diagnostics pour les traductions publiques uniquement

Pour accéder aux diagnostics pour une instance, à partir de l'onglet NAT, cliquez sur l'ellipse dans la colonne Diagnostics.



La boîte de dialogue NAT Diagnostics affiche les diagnostics de l'instance sélectionnée.

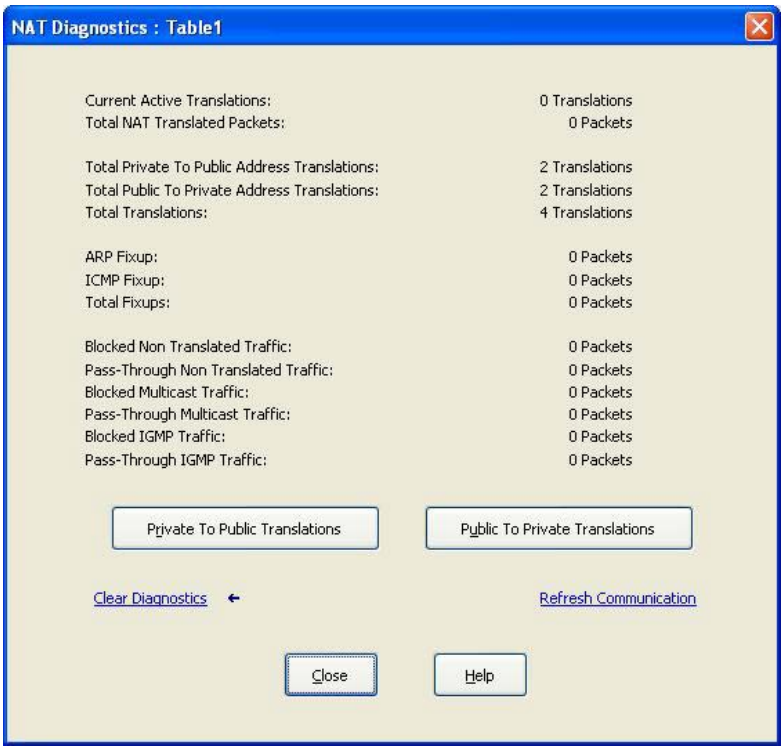


Tableau 42 - Diagnostic NAT par Instance

Champ	Description
Current Active Translations (traductions actives actuelles)	Affiche le nombre de traductions survenues dans les 90 dernières secondes sur toutes les instances NAT.
Total NAT Translated Packets (paquets NAT traduits totaux)	Affiche le nombre total de paquets qui ont été traduits pour cette instance.
Total Private to Public Address Translations (traductions d'adresse privée à publique totales)	Affiche le nombre total de traductions de privées-à-publiques pour cette instance.
Total Private to Public Address Translations (traductions d'adresse publique à privée totales)	Affiche le nombre total de traductions de public-à-privé pour cette instance.
ARP Fixup (correction ARP)	Affiche le nombre de paquets ARP corrigés pour cette instance.
ICMP Fixup (correction ICMP)	Affiche le nombre de paquets ICMP corrigés pour cette instance.

Tableau 42 - Diagnostic NAT par Instance (suite)

Champ	Description
Total Fixups (corrections totales)	Affiche le nombre de paquets ARP et ICMP corrigés pour cette instance.
Incoming Non Translated Traffic (trafic entrant non traduit – Pass-Through)	Affiche le nombre de paquets entrants avec un trafic non traduit, que NAT a fait passer pour cette instance.
Outgoing Non Translated Traffic (trafic sortant non traduit – bloqué)	Affiche le nombre de paquets sortants avec trafic non traduit que NAT a bloqués pour cette instance.
Incoming Multicast Traffic (trafic multidiffusion entrant – bloqué)	Affiche le nombre de paquets entrants avec trafic multidiffusion que NAT a bloqués pour cette instance.
Outgoing Multicast Traffic (trafic multidiffusion sortant – Pass-Through)	Affiche le nombre de paquets sortants avec trafic multidiffusion que NAT a fait passer pour cette instance.
Incoming IGMP Traffic (trafic IGM¨entrant – bloqué)	Affiche le nombre de paquets entrants avec trafic IGMP que NAT a bloqués pour cette instance.
Outgoing IGMP Traffic (trafic IGMP sortant – bloqué)	Affiche le nombre de paquets sortants avec trafic IGMP que NAT a bloqués pour cette instance.
Private to Public Translations (traductions privées vers publiques)	Cliquez pour voir les diagnostics de traduction privée-à-publique pour l'instance. Reportez-vous à Diagnostics de traduction privée à publique, à la page 201.
Public to Private Translations (traductions publiques vers privées)	Cliquez pour voir les diagnostics de traduction publique-à-privée pour l'instance. Reportez-vous à Diagnostics de traduction publique à privée, à la page 202.
Refresh Communication (actualiser la communication)	Cliquez pour actualiser tous les diagnostics de cette instance.

Diagnostics de traduction privée à publique

À partir de la boîte de dialogue Private to Public Translations d'une instance, vous pouvez afficher une liste d'adresses IP qui ont été modifiées par NAT dans les 90 dernières secondes.

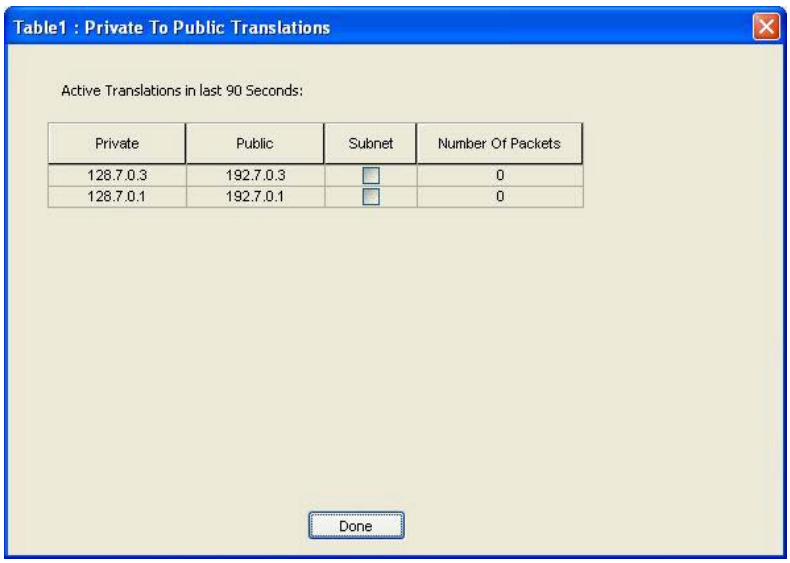


Tableau 43 - Diagnostics de traduction privée à publique

Champ	Description
Private (privé)	Affiche l'adresse existante pour un dispositif sur le sous-réseau privé.
Public (publique)	Affiche une adresse publique unique qui représente le dispositif correspondant sur le sous-réseau privé.
Subnet (sous-réseau)	Indique si la traduction fait partie d'un type de saisie de sous-réseau.
Number of Packets (nbre de paquets)	Affiche le nombre de paquets qui contiennent la traduction.

Diagnostics de traduction publique à privée

À partir de la boîte de dialogue Public to Private Translation d'une instance, vous pouvez afficher une liste d'adresses IP qui ont été modifiées par NAT dans les 90 dernières secondes.

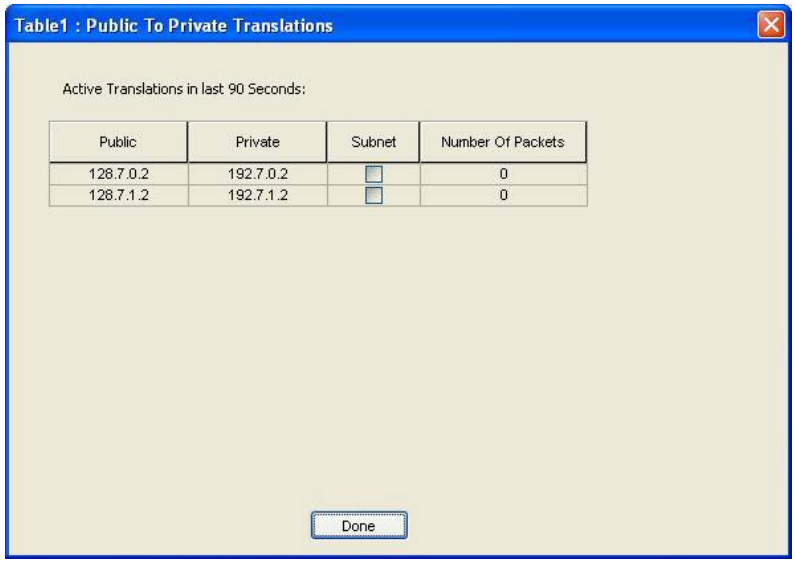


Tableau 44 - Diagnostics de traduction publique à privée

Champ	Description
Public (publique)	Affiche l'adresse IP unique du sous-réseau public qui représente l'adresse IP correspondante sur le sous-réseau privé.
Private (privé)	Affiche l'adresse IP du sous-réseau privé qui a été modifiée en une adresse IP unique sur le sous-réseau public.
Subnet (sous-réseau)	Indique si la traduction fait partie d'un type de saisie de sous-réseau.
Number of Packets (nbre de paquets)	Affiche le nombre de paquets qui contiennent la traduction.

Flash Sync de la caret SD

Vous pouvez synchroniser la carte SD avec le fichier de configuration ou l'ensemble de l'image.

IMPORTANT Vous pouvez écraser votre configuration si vous synchronisez dans la mauvaise direction.

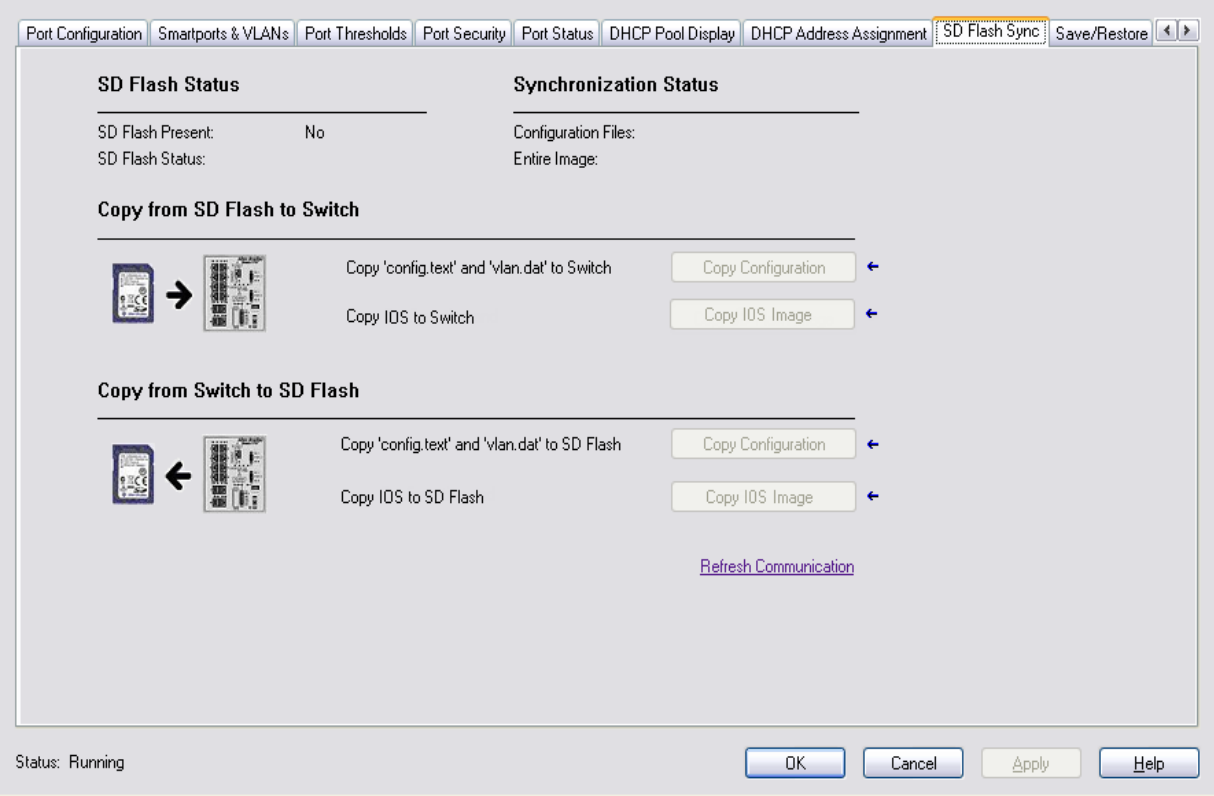


Tableau 45 - Champs de l'onglet SD Flash Sync

Champ	Description
SD Flash Status (état Flash SD)	Indique si la carte SD est présente et l'état de la carte.
Synchronization Status (état de synchronisation)	Indique si l'IOS et les fichiers de configuration sont synchronisés ou non.
Copy from SD Flash to Switch (copier de Sd Flash vers le switch)	Choisissez parmi les options suivantes : • Copy Configuration (copier la configuration) • Copy IOS Image (copier l'image IOS)
Copy from Switch to SD Flash (copier du switch vers SD Flash)	Choisissez parmi les options suivantes : • Copy Configuration (copier la configuration) • Copy IOS Image (copier l'image IOS)

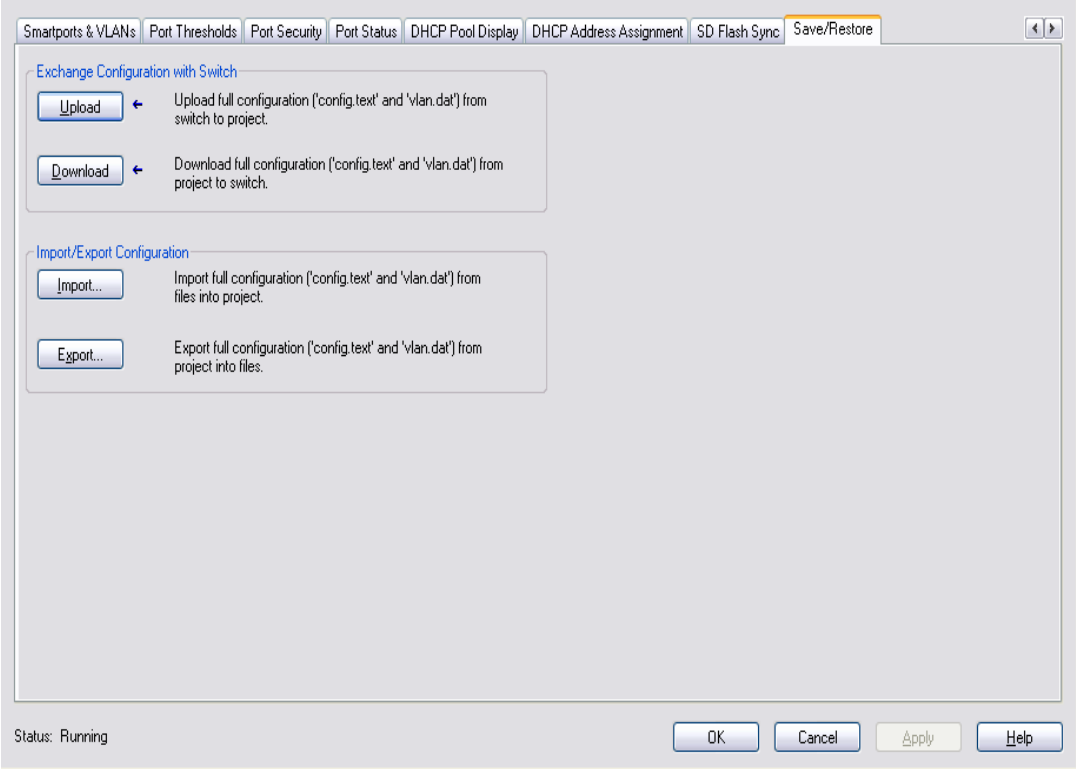
Sauvegarde et restauration de la configuration du switch

Utilisez cet onglet pour effectuer les opérations suivantes :

- Sauvegarder la configuration du switch sur un fichier à des fins d'archivage
- Restaurer une configuration de switch stockée localement sur l'ordinateur ou à l'intérieur du projet d'application Logix Designer.

Vous devez être en ligne pour sauvegarder et restaurer les fichiers de configuration. La plupart des réglages apparaissent en grisé lorsque le switch est hors ligne.

Préparez-vous à entrer un mot de passe valable pour sauvegarder et restaurer une configuration du switch.



La configuration du switch se compose de ces deux fichiers :

- Fichier texte contenant des paramètres de configuration
- Fichier binaire contenant des informations VLAN

Une fois la configuration du switch téléchargée dans le fichier de projet de l'application Logix Designer, elle peut être exportée en tant que fichier d'ordinateur via le bouton Export.

Vous pouvez importer une configuration de switch à partir des fichiers correspondants de votre ordinateur en utilisant le bouton Import sur l'AOP du switch. Vous pouvez ensuite télécharger la configuration sur le switch en utilisant le bouton Download sur l'AOP. Reportez-vous à Sauvegarde et restauration de la configuration du switch, à la page 204 Pour plus d'informations sur la fonction Save and Restore.

Dépannage du switch

Ce chapitre a pour but de vous aider à résoudre les problèmes liés aux switchs Stratix 5700, ainsi qu'à exécuter des fonctions courantes telles que la réinitialisation du switch.

Pour des instructions de dépannage supplémentaires, reportez-vous aux sections suivantes :

- Diagnostic des problèmes de câblage à la page 151
- Affichage des messages du journal système à la page 152

Vérifier l'amorçage rapide

Les erreurs d'amorçage rapide peuvent provoquer des dégâts irrémédiables au switch. Contactez votre représentant Rockwell Automation si votre switch ne passe pas avec succès l'amorçage rapide. Vous pouvez désactiver l'amorçage rapide et effectuer une auto vérification au démarrage (POST) à l'aide de l'interface de ligne de commande.

Problèmes d'adresse IP

Voici quelques conseils de dépannage de base pour les problèmes d'adresse IP du switch.

Problème	Résolution
L'adresse IP n'a pas été reçue depuis le serveur DHCP	Si le switch ne reçoit pas d'adresse IP d'un dispositif en amont fonctionnant comme un serveur DHCP, assurez-vous que le dispositif en amont fonctionne comme un serveur DHCP et suivez de nouveau les procédures de configuration du switch décrites au Chapitre 1, À propos des switchs.
L'adresse IP du switch est erronée	Si le switch est installé sur votre réseau, mais que vous ne pouvez accéder au switch car son adresse IP est erronée, attribuez une nouvelle adresse IP au switch. Reportez-vous à Accès au mode de gestion directe, à la page 207 pour attribuer l'adresse IP, puis mettez à jour l'adresse IP du switch dans la fenêtre Express Setuo de Device Manager.

Problèmes avec l'interface Internet de Device Manager

Voici quelques instructions de dépannage de base pour les problèmes d'affichage de l'interface Internet de Device Manager.

Problème	Résolution
L'interface Internet de Device Managerne s'affiche pas	Si vous ne pouvez pas afficher l'interface Internet de Device Manager sur votre ordinateur ou sur votre ordinateur portable, assurez-vous que vous avez correctement saisi l'adresse IP du switch dans le navigateur. Si vous avez correctement saisi l'adresse IP du switch dans le navigateur, assurez-vous que le switch et votre ordinateur de bureau ou votre ordinateur portable se trouvent sur le même réseau ou sous-réseau : • Par exemple, si l'adresse IP de votre switch est 172.20.20.85 et celle de votre ordinateur de bureau ou ordinateur portable est 172.20.20.84, les deux appareils sont sur le même réseau. • Par exemple, si l'adresse IP de votre switch est 172.20.20.85 et celle de votre ordinateur de bureau ou ordinateur portable est 10.0.0.2, les deux appareils sont sur des réseaux différents et ne peuvent pas communiquer directement sans un routeur. Vous devez modifier l'adresse IP du switch ou celle de l'ordinateur de bureau ou de l'ordinateur portable. • Si le problème persiste, suivez la procédure indiquée à la section Accès au mode de gestion directe en page 207, puis mettez à jour les réglages de réseau du switch dans la fenêtre Express Setup de Device Manager. • Si le problème persiste, suivez la procédure indiquée dans la section Récupérer le firmware du switch et restaurer les valeurs par défaut en page 210.
L'interface Internet de Device Manager ne fonctionne pas correctement	Si l'interface Internet de Device Manager ne fonctionne pas correctement (par exemple, Device Manager ne répond pas), suivez la procédure indiquée dans la section Accès au mode de gestion directe en page 207, puis mettez à jour les réglages de réseau du switch dans la fenêtre Express Setup de l'interface Internet de Device Manager. Si le problème persiste, suivez la procédure indiquée dans la section Récupérer le firmware du switch et restaurer les valeurs par défaut en page 210.
L'interface Internet de Device Manager n'est pas accessible par l'intermédiaire du réseau	Si vous ne pouvez pas accéder à Device Manager à distance depuis un navigateur Internet, suivez la procédure indiquée dans la section Accès au mode de gestion directe en page 207.

Performances du switch

Voici quelques instructions de dépannage de base pour les problèmes de performance du switch.

Problème	Résolution
Vitesse, Duplex et Négociation automatique	Si les statistiques de port montrent une grande quantité d'erreurs d'alignement, de séquence de contrôle de trame (FCS) ou de collisions tardives, cela peut indiquer une incompatibilité de vitesse ou de duplex. Un problème habituel avec la vitesse et le duplex survient lorsque les réglages de duplex sont discordant entre les deux switchs, entre un switch et un routeur, ou entre le switch et un poste de travail ou un serveur. Cela peut se produire suite au réglage manuel de la vitesse et du duplex ou à des problèmes de négociation automatique entre les deux dispositifs. Une discordance se produit dans les circonstances suivantes : • Un paramètre de vitesse ou de duplex défini manuellement diffère du paramètre de vitesse ou de duplex défini manuellement sur le port connecté. • Un port est configuré pour la négociation automatique et le port connecté est défini sur duplex intégral sans négociation automatique. Pour optimiser les performances du switch et assurer une liaison, suivez l'une des consignes ci-dessous lors du changement des réglages de vitesse et de duplex : • Laissez les ports négocier automatiquement aussi bien la vitesse que le duplex. • Définissez manuellement les mêmes valeurs de paramètres de vitesse et de duplex sur les ports aux deux extrémités de la connexion. • Si un dispositif distant n'effectue pas de négociation automatique, configurez les réglages de duplex des deux ports sur les mêmes valeurs. Le paramètre de vitesse peut s'ajuster automatiquement même si le port connecté n'applique pas de négociation automatique.
Négociation automatique et cartes d'interface réseau (cartes réseau)	Des problèmes surviennent parfois entre le switch et des cartes d'interface réseau tierces. Par défaut, les interfaces et ports du switch sont réglés de manière à effectuer une négociation automatique. Bien que les périphériques tels que les ordinateurs portables ou autres appareils soient généralement réglés sur négociation automatique, des problèmes de négociation automatique peuvent se présenter. Pour résoudre les problèmes de négociation automatique, essayez de configurer manuellement les deux côtés de la connexion. Si cela ne résout pas le problème, il peut y avoir un problème au niveau du firmware ou du logiciel de votre carte réseau. Vous pouvez résoudre ce problème en mettant à niveau le driver de la carte réseau avec le dernier firmware ou logiciel disponible auprès du fabricant.
Distance de câblage	Si les statistiques de port affichent des erreurs excessives de FCS, de collision tardive ou d'alignement, vérifiez que la distance de câblage entre le switch et le dispositif connecté satisfait aux consignes recommandées.

Accès au mode de gestion directe

Vous pouvez afficher l'interface Internet de Device Manager et gérer le switch grâce à une connexion physique entre l'un des ports du switch et votre ordinateur de bureau ou ordinateur portable. Ce type de connexion de gestion est appelé Mode de gestion directe. Ce mode est généralement utilisé pour se connecter au switch via l'interface Internet de Device Manager lorsque l'adresse IP du switch est inconnue.

Avant de pouvoir accéder au Mode de gestion directe, vous devez vérifier les éléments suivants :

- Vous devez disposer d'un accès physique au switch.
- Assurez-vous qu'au moins un port du switch est activé et n'est pas connecté à un dispositif.

Pour accéder au Mode de gestion directe, suivez ces étapes.

1. Appuyez sur le bouton Express Setup jusqu'à ce que le voyant d'état Setup clignote en vert et que le voyant d'état d'un port de liaison descendante disponible sur le switch clignote en vert.

   Le port disposant d'un voyant d'état vert clignotant est désigné comme port du Mode de gestion directe. Ce port est déterminé par les éléments suivants :

   - Si aucun port de liaison descendante n'est connecté à des dispositifs ou si plusieurs ports de liaison descendante sont connectés à des dispositifs, le premier port de liaison descendante disponible est sélectionné comme port du Mode de gestion directe.

- Si un seul port de liaison descendante est connecté à un dispositif, ce port est sélectionné comme port du Mode de gestion directe.

S'il n'existe aucun port de liaison descendante du switch disponible auquel votre ordinateur de bureau ou votre ordinateur portable peut être connecté, débranchez un dispositif de l'un des ports de liaison descendante du switch, puis appuyez de nouveau sur le bouton Setup jusqu'à ce que le voyant d'état Setup et le voyant d'état du port clignotent en vert.

2. Utilisez un câble Ethernet catégorie 5 pour relier votre ordinateur de bureau ou votre ordinateur portable au port du switch dont le voyant d'état est vert clignotant.
3. Attendez que les voyants d'état des ports sur le switch et sur votre ordinateur de bureau ou votre ordinateur portable passent au vert fixe.

   Les voyants d'état verts indiquent une connexion réussie entre les deux dispositifs.
4. Lancez un navigateur Internet sur votre ordinateur de bureau ou votre ordinateur portable.

   Une invite de mot de passe apparaît, suivie de l'interface Internet de Device Manager.

   Si l'interface Internet de Device Manager n'apparaît pas, assurez-vous que les bloqueurs de fenêtres furtives et les réglages de proxy de votre logiciel de navigation sont désactivés et que tous les clients sans fil en cours d'exécution sur votre ordinateur de bureau ou votre ordinateur portable sont désactivés.

   Si l'interface Internet de Device Manager n'apparaît pas, saisissez une URL dans votre navigateur, par exemple http://www.rockwellautomation.com. Le navigateur se redirige vers l'interface Internet de Device Manager.

Redémarrer ou réinitialiser le switch

Si vous ne pouvez pas résoudre un problème en reconfigurant une fonctionnalité, le fait de redémarrer ou réinitialisater le switch peut résoudre le problème ou vous aider à en éliminer les causes probables. Si le problème apparaît après que vous avez réinitialisé le switch à ses réglages par défaut, il est peu probable que le switch soit à l'origine du problème.

Option	Description
Restart (redémarrage)	Cette option permet de redémarrer le switch sans mise hors tension. Le switch conserve ses réglages de configuration enregistrés pendant le processus de redémarrage. Cependant, l'interface Internet de Device Manager n'est pas disponible pendant ce processus. À la fin du processus, le switch affiche l'interface Internet de Device Manager. **IMPORTANT :** le fait de redémarrer le switch interrompt la connexion de vos dispositifs au réseau.
Reset the Switch to Factory Defaults (Réinitialiser le switch aux valeurs par défaut)	Cette option permet de réinitialiser le switch, de supprimer les réglages de configuration actuels, de restaurer les réglages par défaut et de redémarrer le switch. **ATTENTION :** le fait de réinitialiser le switch a pour effet de supprimer tous les réglages personnalisés du switch, y compris l'adresse IP, et de remplacer tous les réglages du switch par les réglages d'usine par défaut. La même image du logiciel est conservée. Vous devez reconfigurer les réglages de base du switch. Reportez-vous à Configuration initiale du switch avec Express Setup, à la page 51. **ATTENTION :** le fait de réinitialiser le switch interrompt la connexion de vos dispositifs avec le réseau.

IMPORTANT Lorsque vous redémarrez ou réinitialisez le switch, la connexion de vos dispositifs avec le réseau est interrompue.

Redémarrer le switch depuis l'interface Internet de Device Manager

Depuis l'interface Internet de Device Manager, dans la boîte de dialogue Restart/Reset, cliquez sur Restart the Switch (redémarrer le switch).

Cette option permet de redémarrer le switch sans mise hors tension. L'interface Internet de Device Manager n'est pas disponible pendant ce processus. À la fin du processus, le switch affiche l'interface Internet de Device Manager.

Si vous ne connaissez pas l'adresse IP du switch, suivez la procédure indiquée dans la section Accès au mode de gestion directe en page 207 pour accéder au mode de gestion directe.

Redémarrer le switch depuis l'application Logix Designer

Effectuez les opérations suivantes depuis la boîte de dialogue Module Properties (Propriétés du module) au sein de l'application Logix Designer.

1. Cliquez sur l'onglet Module Info (Informations sur le module).
2. Cliquez sur Reset Module (Réinitialiser le module).

   Une invite de mot de passe s'affiche.
3. Saisissez votre mot de passe puis cliquez sur Enter (Entrée).

Réinitialiser le switch sur les valeurs d'usine par défaut

ATTENTION : réinitialiser le switch supprime tous les réglages personnalisés du switch, y compris l'adresse IP, et remplace tous les réglages du switch par les réglages d'usine par défaut. La même image du logiciel est conservée. Pour gérer le switch ou pour afficher le gestionnaire de dispositif, vous devez reconfigurer les réglages de base du switch (tel que décrits dans le Chapitre 4, Gestion du switch via l'interface Internet de Device Manager) et utiliser la nouvelle adresse IP.

IMPORTANT Le fait de réinitialiser le switch interrompt la connexion de vos dispositifs avec le réseau.

Procédez comme suit depuis l'interface Internet de Device Manager.

1. Accédez à la boîte de dialogue de redémarrage et de réinitialisation de l'interface Internet de Device Manager.
2. Cliquez sur Reset the Switch (Réinitialiser le switch).

   Cette option permet de réinitialiser le switch, de supprimer les réglages de configuration actuels, de restaurer les réglages par défaut et de redémarrer le switch.

   Si vous ne connaissez pas l'adresse IP du switch, suivez la procédure indiquée dans la section Accès au mode de gestion directe en page 207 pour accéder au mode de gestion directe. Revenez ensuite à l'étape 1 ci-dessus.

Récupérer le firmware du switch et restaurer les valeurs par défaut

Avant de pouvoir récupérer le firmware d'un switch, vous devez vérifier les éléments suivants :

- Vous devez disposer d'un accès physique au switch.
- Assurez-vous qu'au moins un port du switch est activé et n'est pas connecté à un dispositif.

Si l'image est corrompue, vous pouvez récupérer le firmware du switch. L'un des symptômes d'un firmware corrompu est une tentative de redémarrage permanente du switch.

Vous pouvez avoir supprimé l'image en raison d'un échec de mise à niveau du firmware ou avoir oublié le mot de passe du switch.

Récupérer le firmware du switch implique de supprimer tous les réglages de configuration et de restaurer la configuration usine par défaut du switch. Suivez les étapes ci-après pour restaurer la configuration usine par défaut du switch.

1. Vérifiez que le switch est déjà mis sous tension et en marche, puis maintenez bouton Express Setup enfoncé jusqu'à ce que les voyants d'état Setup et EIP Net deviennent rouges.

   Ce processus prend environ 18 à 20 secondes.
2. Relâchez le bouton Express Setup.
3. Attendez que le switch redémarre.

   Le voyant Express Setup commence à clignoter lorsque le switch a terminé son redémarrage. Le switch a désormais été restauré à sa configuration usine par défaut.
4. Configurez le switch de la manière décrite dans la section Configuration initiale du switch avec Express Setup à la page 51.
5. Reportez-vous à Dépanner une mise à niveau du firmware, à la page 210 et suivez la procédure de mise à jour du firmware.

Dépanner une mise à niveau du firmware

Si vous a tenté de mettre à jour le firmware du switch et reçu un message indiquant que la mise à niveau a échoué, vérifiez que vous avez encore accès au switch. Si vous avez encore accès au switch, suivez les étapes ci-après.

1. Assurez-vous que vous avez téléchargé le fichier .tar approprié depuis le site http://www.rockwellautomation.com.
2. Si vous avez téléchargé le fichier .tar approprié, actualisez votre session de navigateur de l'interface Internet de Device Manager pour vous assurer qu'il existe une connectivité entre le switch et votre ordinateur ou ordinateur portable ou votre lecteur réseau.
   - Si vous disposez d'une connectivité vers le switch et l'interface Internet de Device Manager, réessayez la mise à niveau.
   - Si vous n'avez pas de connectivité vers le switch et l'interface Internet de Device Manager, reportez-vous à la section Récupérer le firmware du switch et restaurer les valeurs par défaut en page 210.

Types de données définis par le module

Dans l'application Logix Designer, les points prédéfinis pour les types de données d'entrée et de sortie ont une structure correspondant au switch sélectionné lorsqu'il a été ajouté à l'arborescence des E/S. Ses éléments sont nommés selon les noms des ports.

Vous pouvez désactiver un port de switch en mettant à un (1) le bit correspondant dans le point de sortie. Les bits de sortie sont appliqués chaque fois que le switch reçoit les données de sortie de l'automate lorsque celui-ci est en mode Run (exécution). Lorsque l'automate est en mode Program, les bits de sortie ne sont pas appliqués.

Le port est activé si le bit de sortie correspondant est 0. Si vous activez ou désactivez un port à l'aide de l'interface Internet de Device Manager ou de la ligne de commande, le réglage de port pourra être écrasé par les bits de sortie à l'application suivante. Les bits de sortie ont toujours la priorité, peu importe si l'interface Internet de Device Manager ou CLI a été utilisée pour activer ou désactiver le port.

Les tableaux figurant dans cette annexe répertorient les types de données définis par le module pour les switchs Stratix 5700. Les tableaux contiennent des informations pour l'entrée (indiquée par un I) et la sortie (indiquée par un O).

Type de données d'entrée défini par le module (switchs Go à 6 ports)

AB:STRATIX_5700_6PORT_GB_MANAGED:I:0			
Nom du membre	**Type**	**Style d'affichage par défaut**	**Valeurs valables**
Fault	DINT	Binaire	
AnyPortConnected	BOOL	Décimal	LinkStatus:0
PortFa1_1Connected	BOOL	Décimal	LinkStatus:1
PortFa1_2Connected	BOOL	Décimal	LinkStatus:2
PortFa1_3Connected	BOOL	Décimal	LinkStatus:3
PortFa1_4Connected	BOOL	Décimal	LinkStatus:4
PortGi1_1Connected	BOOL	Décimal	LinkStatus:5
PortGi1_2Connected	BOOL	Décimal	LinkStatus:6
AnyPortUnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:0
PortFa1_1UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:1
PortFa1_2UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:2
PortFa1_3UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:3
PortFa1_4UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:4
PortGi1_1UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:5
PortGi1_2UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:6
AnyPortThreshold	BOOL	Décimal	ThresholdExceeded:0
PortFa1_1Threshold	BOOL	Décimal	ThresholdExceeded:1
PortFa1_2Threshold	BOOL	Décimal	ThresholdExceeded:2
PortFa1_3Threshold	BOOL	Décimal	ThresholdExceeded:3
PortFa1_4Threshold	BOOL	Décimal	ThresholdExceeded:4
PortGi1_1Threshold	BOOL	Décimal	ThresholdExceeded:5
PortGi1_2Threshold	BOOL	Décimal	ThresholdExceeded:6
AllPortsUtilization	SINT	Décimal	
PortFa1_1Utilization	SINT	Décimal	
PortFa1_2Utilization	SINT	Décimal	
PortFa1_3Utilization	SINT	Décimal	
PortFa1_4Utilization	SINT	Décimal	
PortGi1_1Utilization	SINT	Décimal	
PortGi1_2Utilization	SINT	Décimal	
MajorAlarmRelay	BOOL	Décimal	AlarmRelay:0
MulticastGroupsActive	DINT	Binaire	

Type de données de sortie défini par le module (switchs Go à 6 ports)

AB:STRATIX_5700_6PORT_GB_MANAGED:O:0			
Nom du membre	**Type**	**Style d'affichage par défaut**	**Valeurs valables**
AllPortsDisabled	BOOL	Décimal	DisablePort:0
PortFa1_1Disable	BOOL	Décimal	DisablePort:1
PortFa1_2Disable	BOOL	Décimal	DisablePort:2
PortFa1_3Disable	BOOL	Décimal	DisablePort:3
PortFa1_4Disable	BOOL	Décimal	DisablePort:4
PortGi1_1Disable	BOOL	Décimal	DisablePort:5
PortGi1_2Disable	BOOL	Décimal	DisablePort:6

Type de données d'entrée défini par le module (switchs à 6 ports)

AB:STRATIX_5700_6PORT_MANAGED:I:0			
Nom du membre	**Type**	**Style d'affichage par défaut**	**Valeurs valables**
Fault	DINT	Binaire	
AnyPortConnected	BOOL	Décimal	LinkStatus:0
PortFa1_1Connected	BOOL	Décimal	LinkStatus:1
PortFa1_2Connected	BOOL	Décimal	LinkStatus:2
PortFa1_3Connected	BOOL	Décimal	LinkStatus:3
PortFa1_4Connected	BOOL	Décimal	LinkStatus:4
PortFa1_5Connected	BOOL	Décimal	LinkStatus:5
PortFa1_6Connected	BOOL	Décimal	LinkStatus:6
AnyPortUnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:0
PortFa1_1UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:1
PortFa1_2UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:2
PortFa1_3UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:3
PortFa1_4UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:4
PortFa1_5UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:5
PortFa1_6UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:6
AnyPortThreshold	BOOL	Décimal	ThresholdExceeded:0
PortFa1_1Threshold	BOOL	Décimal	ThresholdExceeded:1
PortFa1_2Threshold	BOOL	Décimal	ThresholdExceeded:2
PortFa1_3Threshold	BOOL	Décimal	ThresholdExceeded:3
PortFa1_4Threshold	BOOL	Décimal	ThresholdExceeded:4
PortFa1_5Threshold	BOOL	Décimal	ThresholdExceeded:5
PortFa1_6Threshold	BOOL	Décimal	ThresholdExceeded:6
AllPortsUtilization	SINT	Décimal	
PortFa1_1Utilization	SINT	Décimal	
PortFa1_2Utilization	SINT	Décimal	
PortFa1_3Utilization	SINT	Décimal	
PortFa1_4Utilization	SINT	Décimal	
PortFa1_5Utilization	SINT	Décimal	
PortFa1_6Utilization	SINT	Décimal	
MajorAlarmRelay	BOOL	Décimal	AlarmRelay:0
MulticastGroupsActive	DINT	Binaire	

Type de données de sortie défini par le module (switchs à 6 ports)

AB:STRATIX_5700_6PORT_MANAGED:O:0			
Nom du membre	**Type**	**Style d'affichage par défaut**	**Valeurs valables**
AllPortsDisabled	BOOL	Décimal	DisablePort:0
PortFa1_1Disable	BOOL	Décimal	DisablePort:1
PortFa1_2Disable	BOOL	Décimal	DisablePort:2
PortFa1_3Disable	BOOL	Décimal	DisablePort:3
PortFa1_4Disable	BOOL	Décimal	DisablePort:4
PortFa1_5Disable	BOOL	Décimal	DisablePort:5
PortFa1_6Disable	BOOL	Décimal	DisablePort:6

Type de données d'entrée défini par le module (switchs Go à 10 ports)

AB:STRATIX_5700_10PORT_GB_MANAGED:I:0			
Nom du membre	**Type**	**Style d'affichage par défaut**	**Valeurs valables**
Fault	DINT	Binaire	
AnyPortConnected	BOOL	Décimal	LinkStatus:0
PortFa1_1Connected	BOOL	Décimal	LinkStatus:1
PortFa1_2Connected	BOOL	Décimal	LinkStatus:2
PortFa1_3Connected	BOOL	Décimal	LinkStatus:3
PortFa1_4Connected	BOOL	Décimal	LinkStatus:4
PortFa1_5Connected	BOOL	Décimal	LinkStatus:5
PortFa1_6Connected	BOOL	Décimal	LinkStatus:6
PortFa1_7Connected	BOOL	Décimal	LinkStatus:7
PortFa1_8Connected	BOOL	Décimal	LinkStatus:8
PortGi1_1Connected	BOOL	Décimal	LinkStatus:9
PortGi1_2Connected	BOOL	Décimal	LinkStatus:10
AnyPortUnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:0
PortFa1_1UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:1
PortFa1_2UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:2
PortFa1_3UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:3
PortFa1_4UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:4
PortFa1_5UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:5
PortFa1_6UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:6
PortFa1_7UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:7
PortFa1_8UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:8
PortGi1_1UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:9
PortGi1_2UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:10
AnyPortThreshold	BOOL	Décimal	ThresholdExceeded:0
PortFa1_1Threshold	BOOL	Décimal	ThresholdExceeded:1
PortFa1_2Threshold	BOOL	Décimal	ThresholdExceeded:2
PortFa1_3Threshold	BOOL	Décimal	ThresholdExceeded:3
PortFa1_4Threshold	BOOL	Décimal	ThresholdExceeded:4
PortFa1_5Threshold	BOOL	Décimal	ThresholdExceeded:5
PortFa1_6Threshold	BOOL	Décimal	ThresholdExceeded:6
PortFa1_7Threshold	BOOL	Décimal	ThresholdExceeded:7

AB:STRATIX_5700_10PORT_GB_MANAGED:I:0			
Nom du membre	**Type**	**Style d'affichage par défaut**	**Valeurs valables**
PortFa1_8Threshold	BOOL	Décimal	ThresholdExceeded:8
PortGi1_1Threshold	BOOL	Décimal	ThresholdExceeded:9
PortGi1_2Threshold	BOOL	Décimal	ThresholdExceeded:10
AllPortsUtilization	SINT	Décimal	
PortFa1_1Utilization	SINT	Décimal	
PortFa1_2Utilization	SINT	Décimal	
PortFa1_3Utilization	SINT	Décimal	
PortFa1_4Utilization	SINT	Décimal	
PortFa1_5Utilization	SINT	Décimal	
PortFa1_6Utilization	SINT	Décimal	
PortFa1_7Utilization	SINT	Décimal	
PortFa1_8Utilization	SINT	Décimal	
PortGi1_1Utilization	SINT	Décimal	
PortGi1_2Utilization	SINT	Décimal	
MajorAlarmRelay	BOOL	Décimal	AlarmRelay:0
MulticastGroupsActive	DINT	Binaire	

Type de données de sortie défini par le module (switchs Go à 10 ports)

AB:STRATIX_5700_10PORT_MANAGED:O:0			
Nom du membre	**Type**	**Style d'affichage par défaut**	**Valeurs valables**
AllPortsDisabled	BOOL	Décimal	DisablePort:0
PortFa1_1Disable	BOOL	Décimal	DisablePort:1
PortFa1_2Disable	BOOL	Décimal	DisablePort:2
PortFa1_3Disable	BOOL	Décimal	DisablePort:3
PortFa1_4Disable	BOOL	Décimal	DisablePort:4
PortFa1_5Disable	BOOL	Décimal	DisablePort:5
PortFa1_6Disable	BOOL	Décimal	DisablePort:6
PortFa1_7Disable	BOOL	Décimal	DisablePort:7
PortFa1_8Disable	BOOL	Décimal	DisablePort:8
PortGi1_1Disable	BOOL	Décimal	DisablePort:9
PortGi1_2Disable	BOOL	Décimal	DisablePort:10

Type de données d'entrée défini par le module (switchs à 10 ports)

AB:STRATIX_5700_10PORT_MANAGED:I:0			
Nom du membre	**Type**	**Style d'affichage par défaut**	**Valeurs valables**
Fault	DINT	Binaire	
AnyPortConnected	BOOL	Décimal	LinkStatus:0
PortFa1_1Connected	BOOL	Décimal	LinkStatus:1
PortFa1_2Connected	BOOL	Décimal	LinkStatus:2
PortFa1_3Connected	BOOL	Décimal	LinkStatus:3
PortFa1_4Connected	BOOL	Décimal	LinkStatus:4
PortFa1_5Connected	BOOL	Décimal	LinkStatus:5
PortFa1_6Connected	BOOL	Décimal	LinkStatus:6
PortFa1_7Connected	BOOL	Décimal	LinkStatus:7
PortFa1_8Connected	BOOL	Décimal	LinkStatus:8
PortFa1_9Connected	BOOL	Décimal	LinkStatus:9
PortFa1_10Connected	BOOL	Décimal	LinkStatus:10
AnyPortUnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:0
PortFa1_1UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:1
PortFa1_2UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:2
PortFa1_3UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:3
PortFa1_4UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:4
PortFa1_5UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:5
PortFa1_6UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:6
PortFa1_7UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:7
PortFa1_8UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:8
PortFa1_9UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:9
PortFa1_10UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:10
AnyPortThreshold	BOOL	Décimal	ThresholdExceeded:0
PortFa1_1Threshold	BOOL	Décimal	ThresholdExceeded:1
PortFa1_2Threshold	BOOL	Décimal	ThresholdExceeded:2
PortFa1_3Threshold	BOOL	Décimal	ThresholdExceeded:3
PortFa1_4Threshold	BOOL	Décimal	ThresholdExceeded:4
PortFa1_5Threshold	BOOL	Décimal	ThresholdExceeded:5
PortFa1_6Threshold	BOOL	Décimal	ThresholdExceeded:6
PortFa1_7Threshold	BOOL	Décimal	ThresholdExceeded:7
PortFa1_8Threshold	BOOL	Décimal	ThresholdExceeded:8
PortFa1_9Threshold	BOOL	Décimal	ThresholdExceeded:9
PortFa1_10Threshold	BOOL	Décimal	ThresholdExceeded:10
AllPortsUtilization	SINT	Décimal	
PortFa1_1Utilization	SINT	Décimal	
PortFa1_2Utilization	SINT	Décimal	
PortFa1_3Utilization	SINT	Décimal	
PortFa1_4Utilization	SINT	Décimal	
PortFa1_5Utilization	SINT	Décimal	
PortFa1_6Utilization	SINT	Décimal	
PortFa1_7Utilization	SINT	Décimal	

AB:STRATIX_5700_10PORT_MANAGED:I:0			
Nom du membre	**Type**	**Style d'affichage par défaut**	**Valeurs valables**
PortFa1_8Utilization	SINT	Décimal	
PortFa1_9Utilization	SINT	Décimal	
PortFa1_10Utilization	SINT	Décimal	
MajorAlarmRelay	BOOL	Décimal	AlarmRelay:0
MulticastGroupsActive	DINT	Binaire	

Type de données de sortie défini par le module (switchs à 10 ports)

AB:STRATIX_5700_10PORT_MANAGED:O:0			
Nom du membre	**Type**	**Style d'affichage par défaut**	**Valeurs valables**
AllPortsDisabled	BOOL	Décimal	DisablePort:0
PortFa1_1Disable	BOOL	Décimal	DisablePort:1
PortFa1_2Disable	BOOL	Décimal	DisablePort:2
PortFa1_3Disable	BOOL	Décimal	DisablePort:3
PortFa1_4Disable	BOOL	Décimal	DisablePort:4
PortFa1_5Disable	BOOL	Décimal	DisablePort:5
PortFa1_6Disable	BOOL	Décimal	DisablePort:6
PortFa1_7Disable	BOOL	Décimal	DisablePort:7
PortFa1_8Disable	BOOL	Décimal	DisablePort:8
PortFa1_9Disable	BOOL	Décimal	DisablePort:9
PortFa1_10Disable	BOOL	Décimal	DisablePort:10

Type de données d'entrée défini par le module (switchs Go à 20 ports)

AB:STRATIX_5700_20PORT_GB_MANAGED:I:0			
Nom du membre	**Type**	**Style d'affichage par défaut**	**Valeurs valables**
Fault	DINT	Binaire	
AnyPortConnected	BOOL	Décimal	LinkStatus:0
PortFa1_1Connected	BOOL	Décimal	LinkStatus:1
PortFa1_2Connected	BOOL	Décimal	LinkStatus:2
PortFa1_3Connected	BOOL	Décimal	LinkStatus:3
PortFa1_4Connected	BOOL	Décimal	LinkStatus:4
PortFa1_5Connected	BOOL	Décimal	LinkStatus:5
PortFa1_6Connected	BOOL	Décimal	LinkStatus:6
PortFa1_7Connected	BOOL	Décimal	LinkStatus:7
PortFa1_8Connected	BOOL	Décimal	LinkStatus:8
PortFa1_9Connected	BOOL	Décimal	LinkStatus:9
PortFa1_10Connected	BOOL	Décimal	LinkStatus:10
PortFa1_11Connected	BOOL	Décimal	LinkStatus:11
PortFa1_12Connected	BOOL	Décimal	LinkStatus:12
PortFa1_13Connected	BOOL	Décimal	LinkStatus:13
PortFa1_14Connected	BOOL	Décimal	LinkStatus:14
PortFa1_15Connected	BOOL	Décimal	LinkStatus:15
PortFa1_16Connected	BOOL	Décimal	LinkStatus:16

AB:STRATIX_5700_20PORT_GB_MANAGED:I:0			
Nom du membre	**Type**	**Style d'affichage par défaut**	**Valeurs valables**
PortFa1_17Connected	BOOL	Décimal	LinkStatus:17
PortFa1_18Connected	BOOL	Décimal	LinkStatus:18
PortGi1_1Connected	BOOL	Décimal	LinkStatus:19
PortGi1_2Connected	BOOL	Décimal	LinkStatus:20
AnyPortUnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:0
PortFa1_1UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:1
PortFa1_2UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:2
PortFa1_3UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:3
PortFa1_4UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:4
PortFa1_5UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:5
PortFa1_6UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:6
PortFa1_7UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:7
PortFa1_8UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:8
PortFa1_9UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:9
PortFa1_10UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:10
PortFa1_11UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:11
PortFa1_12UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:12
PortFa1_13UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:13
PortFa1_14UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:14
PortFa1_15UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:15
PortFa1_16UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:16
PortFa1_17UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:17
PortFa1_18UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:18
PortGi1_1UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:19
PortGi1_2UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:20
AnyPortThreshold	BOOL	Décimal	ThresholdExceeded:0
PortFa1_1Threshold	BOOL	Décimal	ThresholdExceeded:1
PortFa1_2Threshold	BOOL	Décimal	ThresholdExceeded:2
PortFa1_3Threshold	BOOL	Décimal	ThresholdExceeded:3
PortFa1_4Threshold	BOOL	Décimal	ThresholdExceeded:4
PortFa1_5Threshold	BOOL	Décimal	ThresholdExceeded:5
PortFa1_6Threshold	BOOL	Décimal	ThresholdExceeded:6
PortFa1_7Threshold	BOOL	Décimal	ThresholdExceeded:7
PortFa1_8Threshold	BOOL	Décimal	ThresholdExceeded:8
PortFa1_9Threshold	BOOL	Décimal	ThresholdExceeded:9
PortFa1_10Threshold	BOOL	Décimal	ThresholdExceeded:10
PortFa1_11Threshold	BOOL	Décimal	ThresholdExceeded:11
PortFa1_12Threshold	BOOL	Décimal	ThresholdExceeded:12
PortFa1_13Threshold	BOOL	Décimal	ThresholdExceeded:13
PortFa1_14Threshold	BOOL	Décimal	ThresholdExceeded:14
PortFa1_15Threshold	BOOL	Décimal	ThresholdExceeded:15
PortFa1_16Threshold	BOOL	Décimal	ThresholdExceeded:16
PortFa1_17Threshold	BOOL	Décimal	ThresholdExceeded:17

AB:STRATIX_5700_20PORT_GB_MANAGED:I:0			
Nom du membre	**Type**	**Style d'affichage par défaut**	**Valeurs valables**
PortFa1_18Threshold	BOOL	Décimal	ThresholdExceeded:18
PortGi1_1Threshold	BOOL	Décimal	ThresholdExceeded:19
PortGi1_2Threshold	BOOL	Décimal	ThresholdExceeded:20
AllPortsUtilization	SINT	Décimal	
PortFa1_1Utilization	SINT	Décimal	
PortFa1_2Utilization	SINT	Décimal	
PortFa1_3Utilization	SINT	Décimal	
PortFa1_4Utilization	SINT	Décimal	
PortFa1_5Utilization	SINT	Décimal	
PortFa1_6Utilization	SINT	Décimal	
PortFa1_7Utilization	SINT	Décimal	
PortFa1_8Utilization	SINT	Décimal	
PortFa1_9Utilization	SINT	Décimal	
PortFa1_10Utilization	SINT	Décimal	
PortFa1_11Utilization	SINT	Décimal	
PortFa1_12Utilization	SINT	Décimal	
PortFa1_13Utilization	SINT	Décimal	
PortFa1_14Utilization	SINT	Décimal	
PortFa1_15Utilization	SINT	Décimal	
PortFa1_16Utilization	SINT	Décimal	
PortFa1_17Utilization	SINT	Décimal	
PortFa1_18Utilization	SINT	Décimal	
PortGi1_1Utilization	SINT	Décimal	
PortGi1_2Utilization	SINT	Décimal	
MajorAlarmRelay	BOOL	Décimal	AlarmRelay:0
MulticastGroupsActive	DINT	Binaire	

Type de données d'entrée défini par le module (switchs Go à 18 ports)

AB:STRATIX_5700_18PORT_GB_MANAGED:I:0			
Nom du membre	**Type**	**Style d'affichage par défaut**	**Valeurs valables**
Fault	DINT	Binaire	
AnyPortConnected	BOOL	Décimal	LinkStatus:0
PortFa1_1Connected	BOOL	Décimal	LinkStatus:1
PortFa1_2Connected	BOOL	Décimal	LinkStatus:2
PortFa1_3Connected	BOOL	Décimal	LinkStatus:3
PortFa1_4Connected	BOOL	Décimal	LinkStatus:4
PortFa1_5Connected	BOOL	Décimal	LinkStatus:5
PortFa1_6Connected	BOOL	Décimal	LinkStatus:6
PortFa1_7Connected	BOOL	Décimal	LinkStatus:7
PortFa1_8Connected	BOOL	Décimal	LinkStatus:8
PortFa1_9Connected	BOOL	Décimal	LinkStatus:9

AB:STRATIX_5700_18PORT_GB_MANAGED:I:0			
Nom du membre	**Type**	**Style d'affichage par défaut**	**Valeurs valables**
PortFa1_10Connected	BOOL	Décimal	LinkStatus:10
PortFa1_11Connected	BOOL	Décimal	LinkStatus:11
PortFa1_12Connected	BOOL	Décimal	LinkStatus:12
PortFa1_13Connected	BOOL	Décimal	LinkStatus:13
PortFa1_14Connected	BOOL	Décimal	LinkStatus:14
PortFa1_15Connected	BOOL	Décimal	LinkStatus:15
PortFa1_16Connected	BOOL	Décimal	LinkStatus:16
PortGi1_1Connected	BOOL	Décimal	LinkStatus:19
PortGi1_2Connected	BOOL	Décimal	LinkStatus:20
AnyPortUnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:0
PortFa1_1UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:1
PortFa1_2UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:2
PortFa1_3UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:3
PortFa1_4UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:4
PortFa1_5UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:5
PortFa1_6UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:6
PortFa1_7UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:7
PortFa1_8UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:8
PortFa1_9UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:9
PortFa1_10UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:10
PortFa1_11UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:11
PortFa1_12UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:12
PortFa1_13UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:13
PortFa1_14UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:14
PortFa1_15UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:15
PortFa1_16UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:16
PortGi1_1UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:19
PortGi1_2UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:20
AnyPortThreshold	BOOL	Décimal	ThresholdExceeded:0
PortFa1_1Threshold	BOOL	Décimal	ThresholdExceeded:1
PortFa1_2Threshold	BOOL	Décimal	ThresholdExceeded:2
PortFa1_3Threshold	BOOL	Décimal	ThresholdExceeded:3
PortFa1_4Threshold	BOOL	Décimal	ThresholdExceeded:4
PortFa1_5Threshold	BOOL	Décimal	ThresholdExceeded:5
PortFa1_6Threshold	BOOL	Décimal	ThresholdExceeded:6
PortFa1_7Threshold	BOOL	Décimal	ThresholdExceeded:7
PortFa1_8Threshold	BOOL	Décimal	ThresholdExceeded:8
PortFa1_9Threshold	BOOL	Décimal	ThresholdExceeded:9
PortFa1_10Threshold	BOOL	Décimal	ThresholdExceeded:10
PortFa1_11Threshold	BOOL	Décimal	ThresholdExceeded:11
PortFa1_12Threshold	BOOL	Décimal	ThresholdExceeded:12
PortFa1_13Threshold	BOOL	Décimal	ThresholdExceeded:13

AB:STRATIX_5700_18PORT_GB_MANAGED:I:0			
Nom du membre	**Type**	**Style d'affichage par défaut**	**Valeurs valables**
PortFa1_14Threshold	BOOL	Décimal	ThresholdExceeded:14
PortFa1_15Threshold	BOOL	Décimal	ThresholdExceeded:15
PortFa1_16Threshold	BOOL	Décimal	ThresholdExceeded:16
PortGi1_1Threshold	BOOL	Décimal	ThresholdExceeded:19
PortGi1_2Threshold	BOOL	Décimal	ThresholdExceeded:20
AllPortsUtilization	SINT	Décimal	
PortFa1_1Utilization	SINT	Décimal	
PortFa1_2Utilization	SINT	Décimal	
PortFa1_3Utilization	SINT	Décimal	
PortFa1_4Utilization	SINT	Décimal	
PortFa1_5Utilization	SINT	Décimal	
PortFa1_6Utilization	SINT	Décimal	
PortFa1_7Utilization	SINT	Décimal	
PortFa1_8Utilization	SINT	Décimal	
PortFa1_9Utilization	SINT	Décimal	
PortFa1_10Utilization	SINT	Décimal	
PortFa1_11Utilization	SINT	Décimal	
PortFa1_12Utilization	SINT	Décimal	
PortFa1_13Utilization	SINT	Décimal	
PortFa1_14Utilization	SINT	Décimal	
PortFa1_15Utilization	SINT	Décimal	
PortFa1_16Utilization	SINT	Décimal	
PortGi1_1Utilization	SINT	Décimal	
PortGi1_2Utilization	SINT	Décimal	
MajorAlarmRelay	BOOL	Décimal	AlarmRelay:0
MulticastGroupsActive	DINT	Binaire	

Type de données de sortie défini par le module (switchs Go à 18 ports)

AB:STRATIX_5700_18PORT_GB_MANAGED:O:0			
Nom du membre	**Type**	**Style d'affichage par défaut**	**Valeurs valables**
AllPortsDisabled	BOOL	Décimal	DisablePort:0
PortFa1_1Disable	BOOL	Décimal	DisablePort:1
PortFa1_2Disable	BOOL	Décimal	DisablePort:2
PortFa1_3Disable	BOOL	Décimal	DisablePort:3
PortFa1_4Disable	BOOL	Décimal	DisablePort:4
PortFa1_5Disable	BOOL	Décimal	DisablePort:5
PortFa1_6Disable	BOOL	Décimal	DisablePort:6
PortFa1_7Disable	BOOL	Décimal	DisablePort:7
PortFa1_8Disable	BOOL	Décimal	DisablePort:8
PortFa1_9Disable	BOOL	Décimal	DisablePort:9
PortFa1_10Disable	BOOL	Décimal	DisablePort:10
PortFa1_11Disable	BOOL	Décimal	DisablePort:11
PortFa1_12Disable	BOOL	Décimal	DisablePort:12
PortFa1_13Disable	BOOL	Décimal	DisablePort:13
PortFa1_14Disable	BOOL	Décimal	DisablePort:14
PortFa1_15Disable	BOOL	Décimal	DisablePort:15
PortFa1_16Disable	BOOL	Décimal	DisablePort:16
PortGi1_1Disable	BOOL	Décimal	DisablePort:19
PortGi1_2Disable	BOOL	Décimal	DisablePort:20

Type de données d'entrée défini par le module (switchs Go à 20 ports)

AB:STRATIX_5700_20PORT_GB_MANAGED:I:0			
Nom du membre	**Type**	**Style d'affichage par défaut**	**Valeurs valables**
Fault	DINT	Binaire	
AnyPortConnected	BOOL	Décimal	LinkStatus:0
PortFa1_1Connected	BOOL	Décimal	LinkStatus:1
PortFa1_2Connected	BOOL	Décimal	LinkStatus:2
PortFa1_3Connected	BOOL	Décimal	LinkStatus:3
PortFa1_4Connected	BOOL	Décimal	LinkStatus:4
PortFa1_5Connected	BOOL	Décimal	LinkStatus:5
PortFa1_6Connected	BOOL	Décimal	LinkStatus:6
PortFa1_7Connected	BOOL	Décimal	LinkStatus:7
PortFa1_8Connected	BOOL	Décimal	LinkStatus:8
PortFa1_9Connected	BOOL	Décimal	LinkStatus:9
PortFa1_10Connected	BOOL	Décimal	LinkStatus:10
PortFa1_11Connected	BOOL	Décimal	LinkStatus:11
PortFa1_12Connected	BOOL	Décimal	LinkStatus:12
PortFa1_13Connected	BOOL	Décimal	LinkStatus:13
PortFa1_14Connected	BOOL	Décimal	LinkStatus:14
PortFa1_15Connected	BOOL	Décimal	LinkStatus:15

AB:STRATIX_5700_20PORT_GB_MANAGED:I:0			
Nom du membre	**Type**	**Style d'affichage par défaut**	**Valeurs valables**
PortFa1_16Connected	BOOL	Décimal	LinkStatus:16
PortFa1_17Connected	BOOL	Décimal	LinkStatus:17
PortFa1_18Connected	BOOL	Décimal	LinkStatus:18
PortGi1_1Connected	BOOL	Décimal	LinkStatus:19
PortGi1_2Connected	BOOL	Décimal	LinkStatus:20
AnyPortUnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:0
PortFa1_1UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:1
PortFa1_2UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:2
PortFa1_3UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:3
PortFa1_4UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:4
PortFa1_5UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:5
PortFa1_6UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:6
PortFa1_7UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:7
PortFa1_8UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:8
PortFa1_9UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:9
PortFa1_10UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:10
PortFa1_11UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:11
PortFa1_12UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:12
PortFa1_13UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:13
PortFa1_14UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:14
PortFa1_15UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:15
PortFa1_16UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:16
PortFa1_17UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:17
PortFa1_18UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:18
PortGi1_1UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:19
PortGi1_2UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:20
AnyPortThreshold	BOOL	Décimal	ThresholdExceeded:0
PortFa1_1Threshold	BOOL	Décimal	ThresholdExceeded:1
PortFa1_2Threshold	BOOL	Décimal	ThresholdExceeded:2
PortFa1_3Threshold	BOOL	Décimal	ThresholdExceeded:3
PortFa1_4Threshold	BOOL	Décimal	ThresholdExceeded:4
PortFa1_5Threshold	BOOL	Décimal	ThresholdExceeded:5
PortFa1_6Threshold	BOOL	Décimal	ThresholdExceeded:6
PortFa1_7Threshold	BOOL	Décimal	ThresholdExceeded:7
PortFa1_8Threshold	BOOL	Décimal	ThresholdExceeded:8
PortFa1_9Threshold	BOOL	Décimal	ThresholdExceeded:9
PortFa1_10Threshold	BOOL	Décimal	ThresholdExceeded:10
PortFa1_11Threshold	BOOL	Décimal	ThresholdExceeded:11
PortFa1_12Threshold	BOOL	Décimal	ThresholdExceeded:12
PortFa1_13Threshold	BOOL	Décimal	ThresholdExceeded:13
PortFa1_14Threshold	BOOL	Décimal	ThresholdExceeded:14
PortFa1_15Threshold	BOOL	Décimal	ThresholdExceeded:15

AB:STRATIX_5700_20PORT_GB_MANAGED:I:0			
Nom du membre	**Type**	**Style d'affichage par défaut**	**Valeurs valables**
PortFa1_16Threshold	BOOL	Décimal	ThresholdExceeded:16
PortFa1_17Threshold	BOOL	Décimal	ThresholdExceeded:17
PortFa1_18Threshold	BOOL	Décimal	ThresholdExceeded:18
PortGi1_1Threshold	BOOL	Décimal	ThresholdExceeded:19
PortGi1_2Threshold	BOOL	Décimal	ThresholdExceeded:20
AllPortsUtilization	SINT	Décimal	
PortFa1_1Utilization	SINT	Décimal	
PortFa1_2Utilization	SINT	Décimal	
PortFa1_3Utilization	SINT	Décimal	
PortFa1_4Utilization	SINT	Décimal	
PortFa1_5Utilization	SINT	Décimal	
PortFa1_6Utilization	SINT	Décimal	
PortFa1_7Utilization	SINT	Décimal	
PortFa1_8Utilization	SINT	Décimal	
PortFa1_9Utilization	SINT	Décimal	
PortFa1_10Utilization	SINT	Décimal	
PortFa1_11Utilization	SINT	Décimal	
PortFa1_12Utilization	SINT	Décimal	
PortFa1_13Utilization	SINT	Décimal	
PortFa1_14Utilization	SINT	Décimal	
PortFa1_15Utilization	SINT	Décimal	
PortFa1_16Utilization	SINT	Décimal	
PortFa1_17Utilization	SINT	Décimal	
PortFa1_18Utilization	SINT	Décimal	
PortGi1_1Utilization	SINT	Décimal	
PortGi1_2Utilization	SINT	Décimal	
MajorAlarmRelay	BOOL	Décimal	AlarmRelay:0
MulticastGroupsActive	DINT	Binaire	

Type de données de sortie défini par le module (switchs Go à 20 ports)

AB:STRATIX_5700_20PORT_GB_MANAGED:0:0			
Nom du membre	**Type**	**Style d'affichage par défaut**	**Valeurs valables**
AllPortsDisabled	BOOL	Décimal	DisablePort:0
PortFa1_1Disable	BOOL	Décimal	DisablePort:1
PortFa1_2Disable	BOOL	Décimal	DisablePort:2
PortFa1_3Disable	BOOL	Décimal	DisablePort:3
PortFa1_4Disable	BOOL	Décimal	DisablePort:4
PortFa1_5Disable	BOOL	Décimal	DisablePort:5
PortFa1_6Disable	BOOL	Décimal	DisablePort:6
PortFa1_7Disable	BOOL	Décimal	DisablePort:7
PortFa1_8Disable	BOOL	Décimal	DisablePort:8
PortFa1_9Disable	BOOL	Décimal	DisablePort:9
PortFa1_10Disable	BOOL	Décimal	DisablePort:10
PortFa1_11Disable	BOOL	Décimal	DisablePort:11
PortFa1_12Disable	BOOL	Décimal	DisablePort:12
PortFa1_13Disable	BOOL	Décimal	DisablePort:13
PortFa1_14Disable	BOOL	Décimal	DisablePort:14
PortFa1_15Disable	BOOL	Décimal	DisablePort:15
PortFa1_16Disable	BOOL	Décimal	DisablePort:16
PortFa1_17Disable	BOOL	Décimal	DisablePort:17
PortFa1_18Disable	BOOL	Décimal	DisablePort:18
PortGi1_1Disable	BOOL	Décimal	DisablePort:19
PortGi1_2Disable	BOOL	Décimal	DisablePort:20

Type de données d'entrée défini par le module (switchs à 20 ports)

AB:STRATIX_5700_20PORT_MANAGED:I:0			
Nom du membre	**Type**	**Style d'affichage par défaut**	**Valeurs valables**
Fault	DINT	Binaire	
AnyPortConnected	BOOL	Décimal	LinkStatus:0
PortFa1_1Connected	BOOL	Décimal	LinkStatus:1
PortFa1_2Connected	BOOL	Décimal	LinkStatus:2
PortFa1_3Connected	BOOL	Décimal	LinkStatus:3
PortFa1_4Connected	BOOL	Décimal	LinkStatus:4
PortFa1_5Connected	BOOL	Décimal	LinkStatus:5
PortFa1_6Connected	BOOL	Décimal	LinkStatus:6
PortFa1_7Connected	BOOL	Décimal	LinkStatus:7
PortFa1_8Connected	BOOL	Décimal	LinkStatus:8
PortFa1_9Connected	BOOL	Décimal	LinkStatus:9
PortFa1_10Connected	BOOL	Décimal	LinkStatus:10
PortFa1_11Connected	BOOL	Décimal	LinkStatus:11
PortFa1_12Connected	BOOL	Décimal	LinkStatus:12
PortFa1_13Connected	BOOL	Décimal	LinkStatus:13
PortFa1_14Connected	BOOL	Décimal	LinkStatus:14

AB:STRATIX_5700_20PORT_MANAGED:I:0			
Nom du membre	**Type**	**Style d'affichage par défaut**	**Valeurs valables**
PortFa1_15Connected	BOOL	Décimal	LinkStatus:15
PortFa1_16Connected	BOOL	Décimal	LinkStatus:16
PortFa1_17Connected	BOOL	Décimal	LinkStatus:17
PortFa1_18Connected	BOOL	Décimal	LinkStatus:18
PortFa1_19Connected	BOOL	Décimal	LinkStatus:19
PortFa1_20Connected	BOOL	Décimal	LinkStatus:20
AnyPortUnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:0
PortFa1_1UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:1
PortFa1_2UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:2
PortFa1_3UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:3
PortFa1_4UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:4
PortFa1_5UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:5
PortFa1_6UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:6
PortFa1_7UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:7
PortFa1_8UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:8
PortFa1_9UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:9
PortFa1_10UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:10
PortFa1_11UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:11
PortFa1_12UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:12
PortFa1_13UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:13
PortFa1_14UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:14
PortFa1_15UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:15
PortFa1_16UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:16
PortFa1_17UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:17
PortFa1_18UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:18
PortFa1_19UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:19
PortFa1_20UnauthorizedDevice	BOOL	Décimal	UnauthorizedDevice:20
AnyPortThreshold	BOOL	Décimal	ThresholdExceeded:0
PortFa1_1Threshold	BOOL	Décimal	ThresholdExceeded:1
PortFa1_2Threshold	BOOL	Décimal	ThresholdExceeded:2
PortFa1_3Threshold	BOOL	Décimal	ThresholdExceeded:3
PortFa1_4Threshold	BOOL	Décimal	ThresholdExceeded:4
PortFa1_5Threshold	BOOL	Décimal	ThresholdExceeded:5
PortFa1_6Threshold	BOOL	Décimal	ThresholdExceeded:6
PortFa1_7Threshold	BOOL	Décimal	ThresholdExceeded:7
PortFa1_8Threshold	BOOL	Décimal	ThresholdExceeded:8
PortFa1_9Threshold	BOOL	Décimal	ThresholdExceeded:9
PortFa1_10Threshold	BOOL	Décimal	ThresholdExceeded:10
PortFa1_11Threshold	BOOL	Décimal	ThresholdExceeded:11
PortFa1_12Threshold	BOOL	Décimal	ThresholdExceeded:12
PortFa1_13Threshold	BOOL	Décimal	ThresholdExceeded:13
PortFa1_14Threshold	BOOL	Décimal	ThresholdExceeded:14

AB:STRATIX_5700_20PORT_MANAGED:I:0			
Nom du membre	**Type**	**Style d'affichage par défaut**	**Valeurs valables**
PortFa1_15Threshold	BOOL	Décimal	ThresholdExceeded:15
PortFa1_16Threshold	BOOL	Décimal	ThresholdExceeded:16
PortFa1_17Threshold	BOOL	Décimal	ThresholdExceeded:17
PortFa1_18Threshold	BOOL	Décimal	ThresholdExceeded:18
PortFa1_19Threshold	BOOL	Décimal	ThresholdExceeded:19
PortFa1_20Threshold	BOOL	Décimal	ThresholdExceeded:20
AllPortsUtilization	SINT	Décimal	
PortFa1_1Utilization	SINT	Décimal	
PortFa1_2Utilization	SINT	Décimal	
PortFa1_3Utilization	SINT	Décimal	
PortFa1_4Utilization	SINT	Décimal	
PortFa1_5Utilization	SINT	Décimal	
PortFa1_6Utilization	SINT	Décimal	
PortFa1_7Utilization	SINT	Décimal	
PortFa1_8Utilization	SINT	Décimal	
PortFa1_9Utilization	SINT	Décimal	
PortFa1_10Utilization	SINT	Décimal	
PortFa1_11Utilization	SINT	Décimal	
PortFa1_12Utilization	SINT	Décimal	
PortFa1_13Utilization	SINT	Décimal	
PortFa1_14Utilization	SINT	Décimal	
PortFa1_15Utilization	SINT	Décimal	
PortFa1_16Utilization	SINT	Décimal	
PortFa1_17Utilization	SINT	Décimal	
PortFa1_18Utilization	SINT	Décimal	
PortFa1_19Utilization	SINT	Décimal	
PortFa1_20Utilization	SINT	Décimal	
MajorAlarmRelay	BOOL	Décimal	AlarmRelay:0
MulticastGroupsActive	DINT	Binaire	

Type de données de sortie défini par le module (switchs à 20 ports)

AB:STRATIX_5700_20PORT_MANAGED:0:0			
Nom du membre	**Type**	**Style d'affichage par défaut**	**Valeurs valables**
AllPortsDisabled	BOOL	Décimal	DisablePort:0
PortFa1_1Disable	BOOL	Décimal	DisablePort:1
PortFa1_2Disable	BOOL	Décimal	DisablePort:2
PortFa1_3Disable	BOOL	Décimal	DisablePort:3
PortFa1_4Disable	BOOL	Décimal	DisablePort:4
PortFa1_5Disable	BOOL	Décimal	DisablePort:5
PortFa1_6Disable	BOOL	Décimal	DisablePort:6
PortFa1_7Disable	BOOL	Décimal	DisablePort:7
PortFa1_8Disable	BOOL	Décimal	DisablePort:8
PortFa1_9Disable	BOOL	Décimal	DisablePort:9
PortFa1_10Disable	BOOL	Décimal	DisablePort:10
PortFa1_11Disable	BOOL	Décimal	DisablePort:11
PortFa1_12Disable	BOOL	Décimal	DisablePort:12
PortFa1_13Disable	BOOL	Décimal	DisablePort:13
PortFa1_14Disable	BOOL	Décimal	DisablePort:14
PortFa1_15Disable	BOOL	Décimal	DisablePort:15
PortFa1_16Disable	BOOL	Décimal	DisablePort:16
PortFa1_17Disable	BOOL	Décimal	DisablePort:17
PortFa1_18Disable	BOOL	Décimal	DisablePort:18
PortFa1_19Disable	BOOL	Décimal	DisablePort:19
PortFa1_20Disable	BOOL	Décimal	DisablePort:20

Affectations de port pour les données CIP

Ce tableau identifie les numéros d'instance de l'objet de liaison Ethernet associé à chaque port sur le switch. L'instance 0 ne s'applique pas à tous les ports, comme elle le fait pour les mappages de bit.

Les numéros de bits identifient chaque port lorsqu'ils sont contenus dans une structure de tous les ports, par exemple dans l'assemblage de sortie. Le bit 0 fait référence à n'importe quel port ou à tous les ports.

Instance/Bit	Switch à 6 ports	Switch Go à 6 ports	Switch à 10 ports	Switch Go à 10 ports	Switch Go à 18 ports	Switch à 20 ports	Switch Go à 20 ports
Bit 0	Tous les ports	Tous les ports	Tous les ports	Tous les ports	Tous les ports	Tous les ports	Tous les ports
Instance/Bit 1	Fa1/1	Fa/1	Fa1/1	Fa1/1	Fa1/1	Fa1/1	Fa1/1
Instance/Bit 2	Fa1/2	Fa1/2	Fa1/2	Fa1/2	Fa1/2	Fa1/2	Fa1/2
Instance/Bit 3	Fa1/3	Fa1/3	Fa1/3	Fa1/3	Fa1/3	Fa1/3	Fa1/3
Instance/Bit 4	Fa1/4	Fa1/4	Fa1/4	Fa1/4	Fa1/4	Fa1/4	Fa1/4
Instance/Bit 5	Fa1/5	Gi1/1	Fa1/5	Fa1/5	Fa1/5	Fa1/5	Fa1/5
Instance/Bit 6	Fa1/6	Gi1/2	Fa1/6	Fa1/6	Fa1/6	Fa1/6	Fa1/6
Instance/Bit 7			Fa1/7	Fa1/7	Fa1/7	Fa1/7	Fa1/7
Instance/Bit 8			Fa1/8	Fa1/8	Fa1/8	Fa1/8	Fa1/8
Instance/Bit 9			Fa1/9	Gi1/1	Fa1/9	Fa1/9	Fa1/9
Instance/Bit 10			Fa1/10	Gi1/2	Fa1/10	Fa1/10	Fa1/10
Instance/Bit 11					Fa1/11	Fa1/11	Fa1/11
Instance/Bit 12					Fa1/12	Fa1/12	Fa1/12
Instance/Bit 13					Fa1/13	Fa1/13	Fa1/13
Instance/Bit 14					Fa1/14	Fa1/14	Fa1/14
Instance/Bit 15					Fa1/15	Fa1/15	Fa1/15
Instance/Bit 16					Fa1/16	Fa1/16	Fa1/16
Instance/Bit 17						Fa1/17	Fa1/17
Instance/Bit 18						Fa1/18	Fa1/18
Instance/Bit 19					Gi1/1	Fa1/19	Gi1/1
Instance/Bit 20					Gi1/2	Fa1/20	Gi1/2
Instance/Bit 27	SVI1	SVI1	SVI1	SVI1	SVI1	SVI1	SVI1

Notes :

Câbles et connecteurs

Ports 10/100 et 10/100/1000

Les ports Ethernet 10/100 et 10/100/1000 sur les switchs utilisent des connecteurs RJ45 standard et brochages Ethernet avec croisements internes.

CONSEIL La fonction auto-MDIX est activée par défaut.

Figure 10 - Brochages des connecteurs 10/100

Broche	Étiquette
1	RD+
2	RD-
3	TD+
4	NC
5	NC
6	TD-
7	NC
8	NC

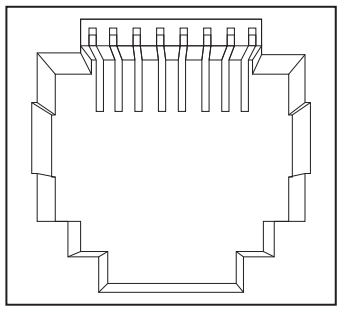
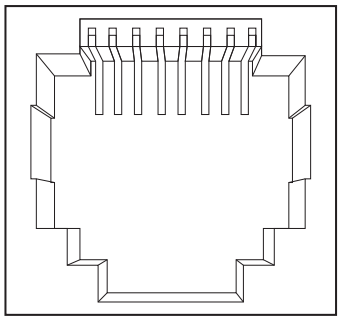


Figure 11 - Brochages des connecteurs 10/100/1000

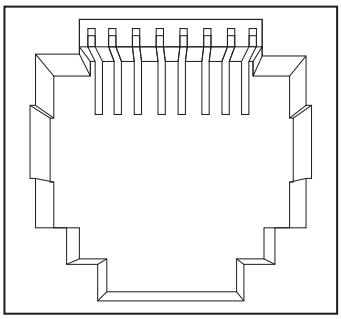
Broche	Étiquette
1	TP0+
2	TP0-
3	TP1+
4	TP2+
5	TP2-
6	TP1-
7	TP3+
8	TP3-



Les ports PoE intègrent les signaux d'alimentation et de données sur les mêmes câbles. Les ports utilisent des connecteurs RJ45 standard et des brochages Ethernet avec croisements internes.

Figure 12 - Brochages des connecteurs 10/100 PoE et tension de l'équipement d'alimentation (PSE)

Broche	Étiquette	Bi-directionnel A (MDI)
1	RD+	V PSE positif
2	RD-	V PSE positif
3	TD+	V PSE négatif
4	NC	
5	NC	
6	TD-	V PSE négatif
7	NC	
8	NC	



Connexion aux dispositifs compatibles 10BASE-T et 100BASE-TX

La fonction auto-MDIX est activée par défaut. Suivez les directives de câblage ci-dessous lorsque la fonction auto-MDIX a été désactivée.

Lorsque vous connectez les ports à des dispositifs compatibles 10BASE-T et 100BASE-TX, tels que des serveurs, des postes de travail et des routeurs, vous pouvez utiliser un câble standard droit à deux ou quatre paires torsadées pour 10BASE-T et 100BASE-TX.

Pour identifier un câble croisé, comparez les deux extrémités modulaires du câble. Maintenez les deux extrémités du câble l'une à côté de l'autre, avec la languette orientée vers l'arrière. Le fil relié à la broche à l'extérieur de la fiche gauche doit être d'une couleur différente de celui qui est branché à la broche à l'intérieur de la fiche droite.

Les figures suivantes illustrent ces schémas :

- Câble direct à deux paires torsadées
- Câble direct à quatre paires torsadées

Figure 13 - Schéma de câble directà deux paires torsadées

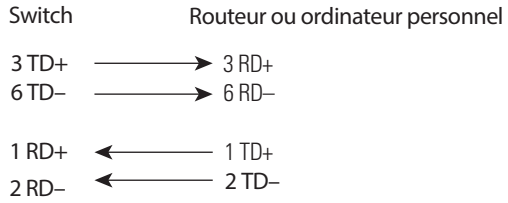
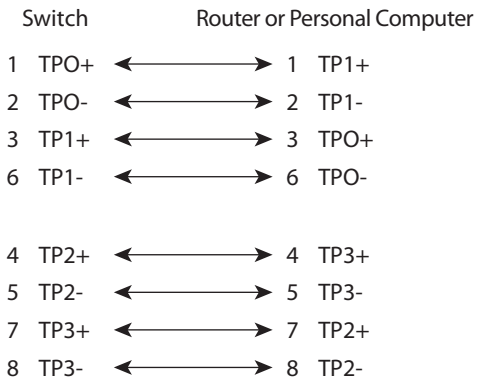


Figure 14 - Schéma de câble direct à quatre paires torsadées



Lorsque vous connectez les ports à des dispositifs compatibles 10BASE-T et 100BASE-TX, tels que des switchs ou des répéteurs, vous pouvez utiliser un câble croisé à deux ou quatre paires torsadées.

Les figures suivantes illustrent ces schémas :

- Schéma de câble croisé à deux paires torsadées
- Schéma de câble croisé à quatre paires torsadées

Utilisez un câble direct pour connecter les deux ports lorsque qu'un seul port est marqué par un X. Utilisez un câble croisé pour relier les deux ports lorsque les deux ports sont marqués par un X ou qu'aucun des deux ne porte un X.

Vous pouvez utiliser des câbles de catégorie 3, 4 ou 5 pour les connexions à des dispositifs compatibles 10BASE-T Vous devez utiliser des câbles de catégorie 5 pour les connexions à des dispositifs compatibles 100BASE-TX.

IMPORTANT Utilisez un câble de catégorie 5 à quatre paires torsadées pour les connexions à un dispositif compatible 1000BASE-T ou un port PoE.

Figure 15 - Schéma de câble croisé à deux paires torsadées

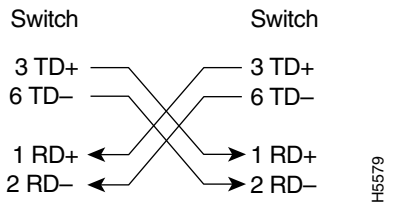
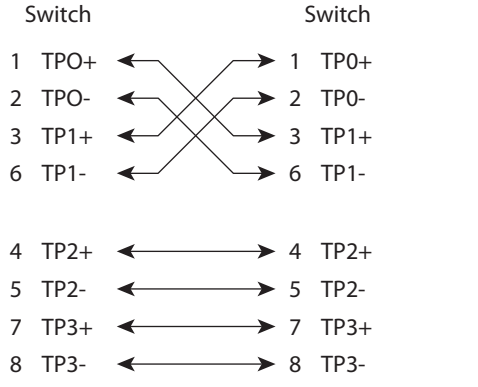


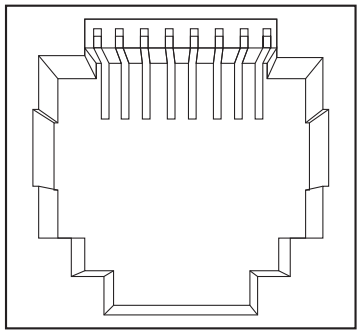
Figure 16 - Schéma de câble croisé à quatre paires torsadées



Ports double fonction (ports mixtes)

Un port Ethernet situé sur un port double fonction utilise des connecteurs RJ45 standard. La figure suivante illustre les brochages.

Figure 17 - Connecteur RJ45 port Ethernet

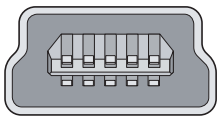
Broche	Étiquette	1 2 3 4 5 6 7 8
1	TP0+	
2	TP0-	
3	TP1+	
4	TP2+	
5	TP2-	
6	TP1-	
7	TP3+	
8	TP3-	

Le logement du module SFP sur un port double fonction utilise des modules SFP pour les ports à fibre optique.

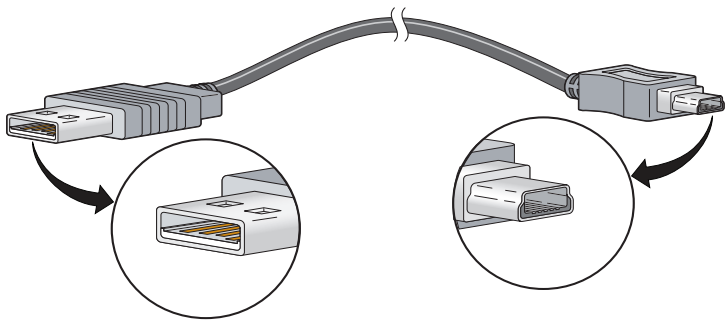
IMPORTANT La fonction auto-MDIX est activée par défaut. Pour obtenir des informations de configuration sur cette fonctionnalité, reportez-vous au guide de configuration logicielle du switch ou à la référence de commande du switch.

Port console

Le switch dispose de deux ports console : un port mini-USB 5 broches de type B sur la face avant et un port console RJ45 sur le panneau arrière. Il ne peut y avoir qu'un port console actif à la fois.

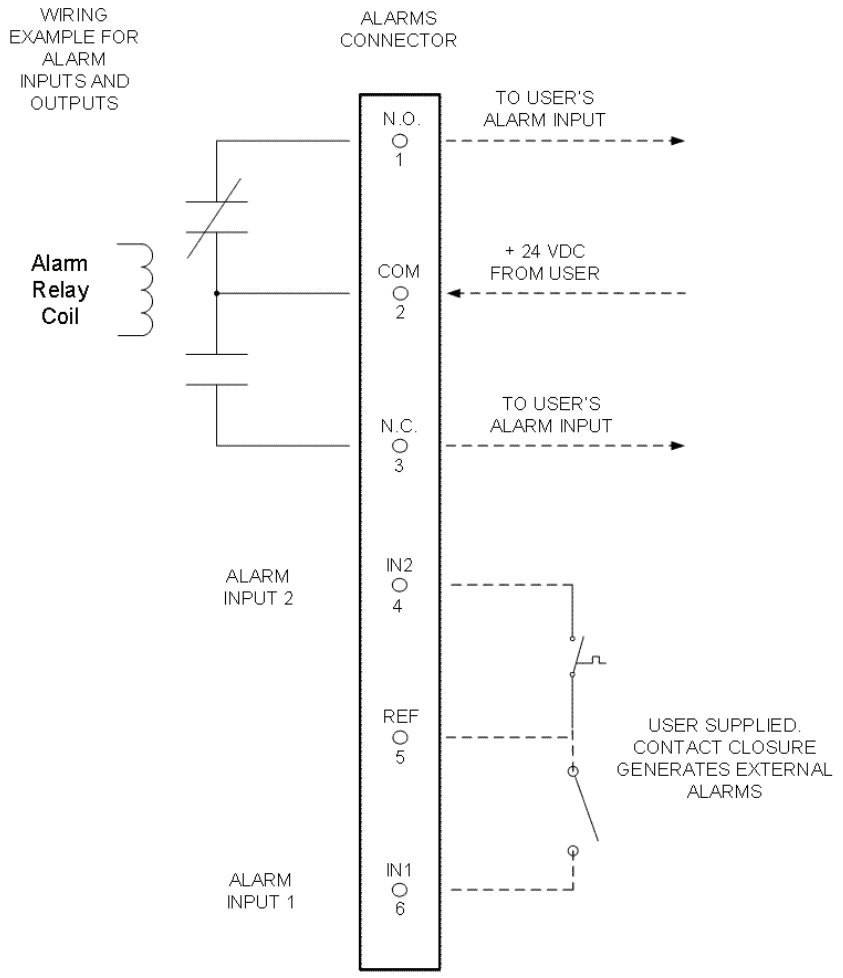


Le port console USB utilise un câble USB type A à mini-USB 5 broches de type B. Le câble USB type A à mini-USB 5 broches de type B n'est pas fourni.



Port d'alarme

Les ports connecteurs relais d'alarme en face avant sont décrits dans le tableau et l'illustration suivants.



Étiquette	Connexion
N.O.	Connexion sortie alarme normalement ouverte (N.O.)
COM	Connexion commun sortie alarme
N.F.	Connexion sortie alarme normalement fermée (N.F.)
IN2	Entrée alarme 2
REF	Connexion référence terre entrée alarme
IN1	Entrée alarme 1

Caractéristiques des câbles et adaptateurs

Ces sections décrivent les câbles et les adaptateurs utilisés avec les switchs.

Spécifications des câbles de modules SFP

Les listes suivantes répertorient les spécifications des câbles de connexion des modules SFP à fibre optique renforcée. Chaque port doit correspondre aux spécifications de longueur d'onde sur l'autre extrémité du câble, et pour une communication fiable, le câble ne doit pas dépasser la longueur maximale nominale.

Tableau 46 - Caractéristiques de câblage des modules SFP à fibre optique

Type de module SFP	Réf.	Longueur d'onde (nm)	Type de fibre	Taille du noyau/du revêtement (micron)	Bande passante modale (MHz/km)(1)	Longueur de câble
100BASE-FX	1783-SFP100FX	1310	MMF	50/125 62,5/125	500 500	2 km 2 km
100BASE-LX	1783-SFP100LX	1310	SMF	G 0,652[2]	—	10 km
1000BASE-SX	1783-SFP1GSX	850	MMF	62,5/125 62,5/125 50/125 50/125	160 200 400 500	220 m 275 m 500 m 550 m
1000BASE-LX/LH	1783-SFP1GLX	1310	SMF	G 0,652[2]	—	10 km

(1) La bande passante modale s'applique uniquement à la fibre multimode.

Caractéristiques de câble port PoE

Pour les ports PoE, utilisez un câble de catégorie 5 (Cat 5) avec une longueur pouvant atteindre 100 m.

Brochages de l'adaptateur

Le tableau suivant répertorie les brochages pour le port console, le câble d'adaptateur RJ45 à DB-9 et le dispositif console.

Tableau 47 - Brochages avec DB 9 broches

Port console du switch (DTE)	Borne adaptateur RJ45 à DB-9	Dispositif console
Signal	**Broche DB 9**	**Signal**
RTS	8	CTS
DTR	6	DSR
TxD	2	RxD
GND	5	GND
GND	5	GND
RxD	3	TxD
DSR	4	DTR
CTS	7	RTS

Le tableau suivant répertorie les brochages pour le port console, l'adaptateur DTE femelle RJ45 à DB-25 et le dispositif console. L'adaptateur DTE femelle RJ45 à DB-25 n'est pas fourni avec le switch.

Tableau 48 - Brochages avec DB 25 broches

Port console du switch (DTE)	Borne adaptateur RJ45 à DB-25	Dispositif console
Signal	**DB 25 broches**	**Signal**
RTS	5	CTS
DTR	6	DSR
TxD	3	RxD
GND	7	GND
GND	7	GND
RxD	2	TxD
DSR	20	DTR
CTS	4	RTS

Notes :

Historique des modifications

Cette annexe résume les révisions apportées à ce manuel. Reportez-vous à cette annexe si vous avez besoin d'informations pour déterminer les modifications effectuées au fil des révisions. Cela peut être particulièrement utile si vous décidez de mettre à niveau votre matériel ou votre logiciel en fonction d'informations ajoutées dans les précédentes révisions de ce manuel.

1783-UM004C-FR-P, décembre 2013

Modification
Accéder aux notes de version du produit
Description des switchs avec Power over Ethernet (PoE)
Dimensions des switchs PoE
Description des ports PoE
Calibre AWG des fils pour le raccordement à la vis de terre externe
Câbler la source d'alimentation PoE
Fixer le connecteur d'alimentation PoE
Se connecter aux ports PoE
Express Setup et carte SD
Numérotation des ports sur les switchs avec PoE
Descriptions de la fonction PoE
Configurer PoE via l'interface Internet de Device Manager
Brochages du connecteur du port PoE et caractéristiques du câble

1783-UM004B-FR-P, juin 2013

Modification
L'application Studio 5000 Logix Designer™ est la nouvelle appelation commerciale du logiciel RSLogix 5000
Description des switchs 1783-BMS10CGN et 1783-BMS20CGN
Identification de la fonctionnalité NAT (Network address translation)
Numérotation des ports pour les switchs 1783-BMS10CGN et 1783-BMS20CGN
Présentation de NAT
Configuration de NAT via l'interface Internet de Device Manager
Surveiller les statistiques NAT via l'interface Internet de Device Manager
Configuration de NAT via l'application Logix Designer
Surveiller les diagnostics NAT via l'application Logix Designer

A

B

C

D

E

F

H

I

J

L

M

N

O

P

R

S

T

V

Assistance Rockwell Automation

Rockwell Automation fournit des informations techniques sur Internet afin de vous aider à utiliser ses produits. Sur le site http://www.rockwellautomation.com/support, vous trouverez des notes techniques et des profils d'application, des exemples de code et des liens vers des mises à jour de logiciels (service pack). Vous pouvez également visiter notre centre d'assistance sur le site https://rockwellautomation.custhelp.com/ pour consulter les foires aux questions, des informations techniques, l'assistance en ligne et les forums, les mises à jour logicielles. Vous pouvez également vous y inscrire pour recevoir les notifications de mise à jour des produits.

En outre, nous offrons de multiples programmes d'assistance pour l'installation, la configuration et le dépannage. Pour de plus amples informations, contactez votre distributeur ou votre représentant Rockwell Automation, ou bien visitez le site http://www.rockwellautomation.com/services/online-phone.

Aide à l'installation

En cas de problème dans les 24 heures suivant l'installation, consultez les informations données dans le présent manuel. Vous pouvez également contacter l'Assistance Rockwell Automation afin d'obtenir de l'aide pour la mise en service de votre produit.

Pour les États-Unis ou le Canada	1-440-646-3434
Pour les autres pays	Utilisez Worldwide Locator à l'adresse http://www.rockwellautomation.com/rockwellautomation/support/overview.page ou contactez votre représentant Rockwell Automation.

Procédure de retour d'un nouveau produit

Rockwell Automation teste tous ses produits pour en garantir le parfait fonctionnement à leur sortie d'usine. Cependant, si votre produit ne fonctionne pas et doit faire l'objet d'un retour, suivez les procédures ci-après.

Pour les États-Unis	Contactez votre distributeur. Vous devrez lui fournir le numéro de dossier que le Centre d'assistance vous aura communiqué (appelez le numéro de téléphone ci-dessus), afin de procéder au retour.
Pour les autres pays	Contactez votre représentant local Rockwell Automation pour savoir comment procéder.

Commentaires sur la documentation

Vos commentaires sur ce document nous aident à mieux vous servir. Si vous avez des suggestions sur la façon d'améliorer ce document, remplissez le formulaire de la publication RA-DU002, disponible sur le site http://www.rockwellautomation.com/literature/.

Rockwell Automation maintient les informations environnementales de ses produits sur son site Internet à l'adresse http://www.rockwellautomation.com/rockwellautomation/about-us/sustainability-ethics/product-environmental-compliance.page.

www.rockwellautomation.com

Siège des activités « Power, Control and Information Solutions »

Amériques : Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 Etats-Unis, Tél: +1 414.382.2000, Fax : +1 414.382.4444
Europe / Moyen-Orient / Afrique : Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgique, Tél: +32 2 663 0600, Fax : +32 2 663 0640
Asie Pacifique : Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tél: +852 2887 4788, Fax : +852 2508 1846

Canada : Rockwell Automation, 3043 rue Joseph A. Bombardier, Laval, Québec, H7P 6C5, Tél: +1 (450) 781-5100, Fax: +1 (450) 781-5101, www.rockwellautomation.ca
France : Rockwell Automation SAS – 2, rue René Caudron, Bât. A, F-78960 Voisins-le-Bretonneux, Tél: +33 1 61 08 77 00, Fax : +33 1 30 44 03 09
Suisse : Rockwell Automation AG, Av. des Baumettes 3, 1020 Renens, Tél: 021 631 32 32, Fax: 021 631 32 31, Customer Service Tél: 0848 000 278

Publication 1783-UM004D-FR-P - Mars 2014