Manuel d’administration des commutateurs du châssis Sun Fire™ B1600 pour serveurs Blade

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054 U.S.A.
650-960-1300

Référence : 817-1892-10
Avril 2003, révision A

Envoyez vos remarques concernant ce document à l'adresse : docfeedback@sun.com

Papier
recyclable

Adobe PostScript

Table des matières

Préface

Le présent *Manuel d'administration des commutateurs du châssis Sun Fire™ B1600 pour serveurs Blade* propose des informations vous permettant de comprendre et d'utiliser le commutateur situé à l'intérieur du module SSC (commutateur et contrôleur système) du châssis. Le commutateur possède deux interfaces : une interface de ligne de commande et une interface Web. Le présent manuel décrit les deux.

Le présent manuel est destiné aux administrateurs réseau responsables de la gestion du châssis. Il suppose une connaissance pratique des opérations effectuées sur les réseaux locaux et une bonne connaissance des protocoles réseau.

Avant de consulter ce manuel

Avant de commencer la configuration du commutateur :

Installez votre châssis conformément aux instructions du *Manuel d'installation des composants du châssis Sun Fire™ B1600 pour serveurs Blade* et du *Manuel d'installation du logiciel du châssis Sun Fire™ B1600 pour serveurs Blade.*

Organisation de ce manuel

Le chapitre 1 présente un aperçu du commutateur, et notamment les options de gestion, les caractéristiques matérielles, les fonctions de commutation et les paramètres par défaut.

Le chapitre 2 décrit comment se connecter à la console du commutateur et à l'interface Web alternative.

Le chapitre 3 décrit toutes les fonctions-clés du commutateur et vous indique comment configurer celles-ci à l'aide de l'interface Web et de l'interface de la console. Il propose également une liste des variables MIB comparables utilisées par les applications de gestion SNMP.

Le chapitre 4 fournit une liste détaillée de toutes commandes et de tous les paramètres de l'interface de la console.

L'annexe A répertorie les bases d'informations de gestion (MIB) ainsi que les interruptions prises en charge par le commutateur.

L'annexe B fournit des informations de base sur le dépannage, et notamment des éléments permettant d'interpréter les voyants système et port, de résoudre des problèmes pouvant vous empêcher d'accéder à l'interface de gestion ainsi que des informations vous permettant d'utiliser les journaux système.

L'annexe C fournit des spécifications détaillées sur les fonctions du commutateur.

Le glossaire définit une liste de termes et d'expressions.

L'index fournit les références aux pages pour les principaux sujets abordés dans ce manuel.

Conventions typographiques

Mise en forme	Signification	Exemples
`AaBbCc123`	Noms des commandes et fichiers ; sorties d'ordinateur sur écran	Affiche les informations système Utilisez `dir` pour répertorier tous les fichiers.
`AaBbCc123`	Données saisies par l'utilisateur devant être différenciées des sorties d'ordinateur sur écran	`>`**`enable`** `Password:`
AaBbCc123	Titres de manuels, termes nouveaux ou mis en évidence Remplace les variables de ligne de commande par des valeurs ou noms existants.	Consultez le chapitre 6 du *Manuel d'installation et de maintenance Sun Fire™ B1600*. Ces options sont appelées options de *classe*. Vous *devez* être connecté en tant qu'administrateur pour pouvoir y accéder. Pour supprimer un fichier, tapez `del` *nom_du_fichier*.

Documentation connexe

Application	Titre	Référence
Installation	*Manuel d'installation des composants du châssis Sun Fire™ B1600 pour serveurs Blade*	817-1903
Installation du logiciel du châssis	*Manuel d'installation du logiciel du châssis pour serveurs Blade*	817-1887
Administration du châssis	*Sun Fire™ B1600 Manuel d'administration du châssis pour serveurs Blade*	817-1897

Accès à la documentation en ligne Sun

De nombreux documents concernant les systèmes Sun sont disponibles à l'adresse suivante :

`http://www.sun.com/products-n-solutions/hardware/docs`

La documentation relative au logiciel Solaris ainsi que d'autres documents sont disponibles à l'adresse :

`http://docs.sun.com`

Commande de documentation Sun

Fatbrain.com, une librairie professionnelle accessible sur Internet, propose une sélection de documentations produits de Sun Microsystems, Inc.

`Avril 2003http://www.fatbrain.com/documentation/sun`

Vos commentaires sont les bienvenus

Dans le but d'améliorer sa documentation, Sun vous invite à lui faire part de vos commentaires et suggestions. Vous pouvez envoyer vos commentaires à l'adresse :

`docfeedback@sun.com`

Mentionnez le numéro de référence de votre documentation (817-1892-10) dans l'objet de votre message électronique.

PART I Avant de commencer

Cette section propose un aperçu du Châssis Sun Fire™ B1600 pour serveurs Blade et présente quelques concepts de base relatifs aux commutateurs réseau. Elle décrit également les paramètres de base requis pour accéder à l'interface de gestion.

Introduction

Configuration initiale

CHAPITRE **1**

Introduction

Le Châssis Sun Fire™ B1600 pour serveurs Blade englobe deux modules SSC (commutateur et contrôleur système), lesquels comprennent un commutateur Gigabit Ethernet hautes performances. Les 16 ports Gigabit « full duplex » internes de ce commutateur assurent un haut degré de connectivité au sein du châssis, tandis que les huit ports Gigabit « full duplex » externes permettent de raccorder celui-ci à un réseau plus vaste.

1.1 Présentation

Les commutateurs assurent une connectivité Gigabit Ethernet au Châssis Sun Fire™ B1600 pour serveurs Blade. Si l'un des commutateurs tombe en panne, le système continue à fonctionner sans interruption sur le second. Tous les composants du châssis - les serveurs Blade, les modules SSC et les unités d'alimentation - sont connectés à un même panneau central, ce qui assure une interconnexion optimale entre ceux-ci.

Chacun des 16 serveurs Blade est connecté à un seul port sur chaque commutateur par le biais d'une liaison Gigabit Ethernet représentant la principale source de signaux E/S du serveur. Le commutateur de chacun des modules SSC constitue la matrice Gigabit Ethernet permettant de raccorder entre eux tous les serveurs Blade, en plus des huit liaisons externes assurant la connexion avec le monde extérieur. Chaque serveur Blade est également raccordé au contrôleur système (SC) de chacun des modules SSC par le biais d'une simple liaison série. Le contrôleur système vous permet de gérer et de contrôler les composants du châssis. Il vous donne également accès à l'interface de ligne de commande du commutateur, ainsi qu'à la console de chaque serveur Blade installé sur le châssis.

1.1.1 Architecture du commutateur

Le commutateur emploie une matrice de commutation ultra rapide permettant le transfert simultané de plusieurs paquets avec une faible latence sur tous les ports. Il s'appuie également sur une technologie d'envoi en différé garantissant une intégrité optimale des données. Dans ce mode, l'ensemble du paquet doit être réceptionné dans un tampon situé sur le port et sa validité doit être vérifiée avant transmission. Cette méthode évite la propagation d'erreurs dans l'ensemble du réseau.

1.1.2 Méthodes d'accès à l'application de gestion du commutateur

Un port console série monté à l'aide d'une prise RJ-45 permet d'accéder au contrôleur système à des fins de gestion sur site. Lorsque vous mettez le châssis du système sous tension, l'interface du contrôleur système (SC) s'affiche. Pour accéder à l'interface de ligne de commande relative au commutateur, consultez « Options de configuration », à la page 2-2 ou reportez-vous au *Manuel d'installation du logiciel du châssis Sun Fire™ B1600 pour serveurs Blade*.

Il est également possible d'accéder directement à cette interface à l'aide de telnet, par le biais du port de gestion 100BASE-TX RJ-45 (NETMGT) situé sur le SSC.

Vous pouvez aussi gérer le commutateur en vous connectant à ce port par le biais du réseau avec un navigateur Web ou un logiciel SNMP/RMON.

Lorsque vous utilisez un navigateur Web pour vous connecter, l'accès HTTP fourni par le commutateur revêt la forme d'une interface utilisateur graphique.

Pour consulter les informations fournies par le protocole SNMP, vous pouvez avoir recours à une application de gestion prenant en charge le protocole SNMP et configurée de la manière ad hoc.

1.2 Description du matériel

Le SSC (commutateur et contrôleur système) comprend la carte du commutateur, le contrôleur système (SC), les ventilateurs, de même que les connecteurs des panneaux central et arrière. Le contrôleur système permet de gérer le châssis du serveur et la carte du commutateur. Il régit également les voyants du système, dont des copies sont situées à l'avant ou l'arrière du Châssis Sun Fire™ B1600 pour serveurs Blade.

1.2.1 Ports Ethernet

1.2.1.1 Ports à liaison ascendante

Huit ports RJ-45 externes prennent en charge l'auto-négociation de la vitesse, du mode duplex et du contrôle de flux conformément à la norme IEEE 802.3x. Chaque port peut fonctionner à 10 Mbps, 100 Mbps et 1000 Mbps, en mode « full et semi duplex » et gérer les flux de données de sorte à empêcher le débordement des tampons. Les ports à liaison ascendante peuvent être connectés à d'autres périphériques compatibles 1000BASE-T conformes à la norme IEEE 802.3ab situés à une distance maximale de 100 m et ce, à l'aide d'un câble à paire torsadée de catégorie 5. Ces ports comportent des fonctions MDI/MDI-X automatiques, ce qui vous permet d'utiliser des câbles droits pour toutes les connexions. Les ports à liaison ascendante sont appelés NETP0 - NETP7 dans l'interface de configuration.

Remarque - Remarquez que, lorsque la fonction d'auto-négociation est active, il est possible de définir automatiquement la vitesse, le mode de transmission ainsi que le contrôle du flux pour autant que cette fonction soit également prise en charge par le périphérique connecté. Dans le cas contraire, ces options peuvent être configurées manuellement pour chacune des connexions.

Remarque - L'auto-négociation doit être activée pour la configuration automatique du brochage MDI/MDI-X.

1.2.1.2 Ports internes

Le commutateur comprend également 16 ports Gigabit Ethernet 1000BASE-X internes connectés aux serveurs Blade à l'intérieur du châssis. Ces ports fonctionnent à 1000 Mbps en mode « full duplex ». Ils sont appelés SNP0 - SNP15 dans l'interface de configuration.

Le commutateur comprend également un port 10/100BASE-TX interne appelé NETMGT et connecté au port réseau du contrôleur système et au port de gestion externe situé sur le panneau avant du module SSC par le biais d'un concentrateur externe.

1.2.2 Voyants d'état

Les voyants d'état du commutateur sont situés sur le module SSC. Les ports 1000BASE-T à liaison ascendante ainsi que le port de gestion 10/100BASE-TX situé sur le panneau arrière du module SSC présentent également des voyants permettant de contrôler la liaison et la vitesse.

FIGURE 1-1 Panneau extérieur du SSC

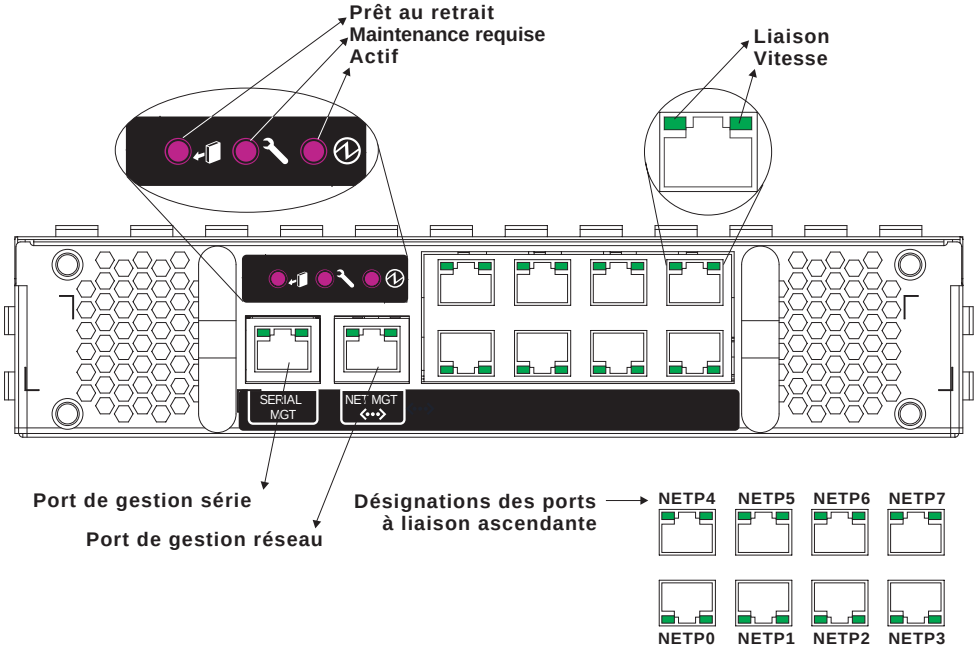


TABLEAU 1-1 Voyants des ports

Voyant	Etat	Statut
SSC		
Actif	Allumé (vert)	Le SSC fonctionne normalement.
Maintenance requise	Allumé (orange)	Le SSC requiert une intervention de maintenance.
Prêt au retrait	Allumé (bleu)	Le SSC peut à présent être retiré.
Ports RJ-45		

TABLEAU 1-1 Voyants des ports

Voyant	Etat	Statut
Liaison	Allumé (vert)	Le port a établi une connexion réseau valable.
Vitesse	Allumé (orange)	La liaison fonctionne à 1 Gbps.
	Eteint	La liaison fonctionne à une vitesse inférieure à 1 Gbps.

1.3 Fonctions du commutateur

Le commutateur propose une vaste gamme de fonctions avancées permettant d'optimiser les performances du système. Le filtrage multidestinataire permet de prendre en charge les applications réseau en temps réel. Les réseaux locaux virtuels (VLAN) basés sur le port et marqués ainsi que la prise en charge de l'enregistrement automatique des VLAN à l'aide du protocole GVRP garantissent un trafic sûr et une utilisation optimale de la bande passante du réseau. Les files d'attente QdS priorisées permettent de réduire au minimum le retard dans le déplacement des données multimédia en temps réel sur le réseau. Le contrôle de flux élimine la perte de paquets imputable à des goulots d'étranglement causés par la saturation des ports. Par ailleurs, la suppression des orages de diffusion empêche l'engorgement du réseau. Certaines de ces fonctions de gestion sont brièvement décrites ci-dessous.

Pont IEEE 802.1D – Le commutateur prend en charge la génération transparente de ponts conformes à la norme IEEE 802.1D. La table d'adressage permet de simplifier la commutation des données grâce à l'apprentissage des adresses, puis au filtrage ou à la transmission du trafic sur la base de ces informations. Cette table peut contenir jusqu'à 8 000 adresses.

Commutation avec envoi différé – Le commutateur copie chaque trame dans sa mémoire avant de la transmettre à un autre port. Cette fonction veille à ce que toutes les trames aient une taille Ethernet standard et que leur exactitude ait été vérifiée à l'aide du contrôle de redondance cyclique (CRC), ce qui empêche la pénétration de trames erronées sur le réseau et le gaspillage de bande passante résultant.

Pour éviter la perte de trames due à la saturation des ports, le commutateur propose un tampon de 128 Ko par port. Celui-ci permet de mettre en attente les paquets qui doivent être transmis sur des réseaux congestionnés.

Protocole Spanning Tree – Le commutateur prend en charge les protocoles Spanning Tree suivants :

Protocole Spanning Tree (STP, IEEE 802.1D) – Ce protocole accroît la tolérance aux pannes en autorisant la création de deux connexions redondantes ou plus entre une paire de segments LAN. Lorsque plusieurs chemins physiques existent entre deux segments, ce protocole en choisit un seul et désactive tous les autres afin de garantir

qu'un seul itinéraire relie deux stations du réseau. Ceci empêche la création de boucles réseau. Toutefois, si une panne survient pour une raison ou une autre, un autre chemin est activé afin de conserver la connexion.

Protocole Spanning Tree Rapide (RSTP, IEEE 802.1w) – Ce protocole réduit le délai de convergence lors des modifications de la topologie du réseau à environ 10 % du temps requis par l'ancienne norme STP IEEE 802.1D. Ce protocole est destiné à remplacer complètement le protocole STP, mais il peut encore fonctionner avec des commutateurs tournant sous l'ancienne norme grâce à la reconfiguration automatique des ports à un mode compatible STP lorsque des messages au protocole STP sont détectés sur les périphériques connectés.

Réseaux locaux virtuels – Le commutateur peut prendre en charge jusqu'à 256 réseaux locaux virtuels (VLAN). Un réseau local virtuel représente un ensemble de noeuds réseau partageant le même domaine de collision indépendamment de leur emplacement physique ou de leur point de connexion au réseau. Le commutateur prend en charge des VLAN marqués basés sur la norme IEEE 802.1Q. Le protocole GVRP permet d'apprendre de manière dynamique quels sont les membres des groupes de réseaux locaux virtuels. Toutefois, il est également possible d'affecter les ports manuellement à un ensemble spécifique de VLAN. Cette fonction permet au commutateur de limiter le trafic aux groupes de VLAN auxquels un utilisateur a été affecté. En segmentant votre réseau en VLAN, vous pouvez :

- éliminer les orages de diffusion qui amoindrissent considérablement les performances d'un réseau plat ;
- simplifier la gestion du réseau en cas de modifications/déplacements de noeuds en configurant l'appartenance aux VLAN à distance pour tous les ports, vous épargnant ainsi la modification manuelle de la connexion réseau ;
- assurer la sécurité des données en limitant tout trafic au VLAN d'origine, à l'exception des cas où une connexion a été configurée entre des VLAN distincts à l'aide d'un routeur ou d'un commutateur de couche 3.

Mise en miroir des ports – Le commutateur peut mettre en miroir le trafic d'un port quelconque vers un port de surveillance sans pour autant en perturber le flux. Vous pouvez alors connecter un analyseur de protocole ou une sonde RMON à ce port afin d'analyser le trafic et de vérifier l'intégrité de la connexion.

Agrégation des ports – Les ports peuvent être combinés en une connexion unique. Il est possible de configurer les groupes de manière manuelle ou dynamique à l'aide du protocole LACP (Link Aggregation Control Protocol) IEEE 802.3ad. Les ports supplémentaires accroissent de manière considérable le débit de toutes les connexions et assurent la redondance en se répartissant le trafic si un port du groupe est défaillant. Le commutateur prend en charge jusqu'à six groupes, avec un maximum de quatre ports à liaison ascendante ou de deux ports à liaison descendante par groupe.

Sécurité des ports – La sécurité des ports empêche les utilisateurs non autorisés d'accéder à votre réseau. Cette fonction permet à chaque port d'apprendre ou de recevoir une liste d'adressage MAC des périphériques autorisés à accéder au réseau

par son biais. Tous les paquets reçus sur le port doivent posséder une adresse source figurant dans la liste autorisée, sans quoi ils sont perdus. Par défaut, la sécurité des ports est désactivée sur tous les ports, mais elle peut être activée sur une base individuelle.

Suppression de la diffusion – Cette fonction empêche le trafic de diffusion de surcharger le réseau. Lorsque cette fonction est activée sur un port, le trafic de diffusion transitant par ce port est limité. Si le trafic de diffusion dépasse un seuil prédéfini, il est ralenti jusqu'à ce que le niveau retombe sous le seuil.

Contrôle de flux – Le contrôle de flux réduit le trafic en cas de congestion et empêche la perte de paquets en cas de débordement du tampon situé sur le port. Le commutateur prend en charge le contrôle de flux basé sur la norme IEEE 802.3x. Par défaut, le contrôle de flux est désactivé sur tous les ports.

Priorité du trafic – Ce commutateur assure la qualité du service (QdS) en priorisant chaque paquet sur la base du niveau de service requis. Pour ce faire, il a recours à la mise en attente WRR (Weighted Round Robin) à tour de rôle dans quatre files priorisées. Le commutateur utilise les marques IEEE 802.1p et 802.1Q pour prioriser le trafic entrant sur la base des informations fournies depuis l'application de station terminale. Ces fonctions peuvent également proposer des priorités indépendantes pour les données sensibles au retard et les données non urgentes.

Ce commutateur prend également en charge plusieurs méthodes courantes de priorisation du trafic de couche 3/4 afin de répondre aux exigences des applications. Les priorités du trafic peuvent être définies sur la base des bits de priorité de l'octet TdS (Type de Service) de la trame IP. Lorsque ces services sont activés, les priorités sont affectées à une valeur Classe de service par le commutateur, et le trafic est alors envoyé à la file d'attente de sortie correspondante.

Filtrage des adresses – Le commutateur propose un filtrage des paquets pour tout trafic pénétrant sur le port de l'unité centrale, et donc potentiellement transmis ou acheminés vers le réseau de gestion. Ce filtrage est basé sur des règles/schémas et constitue un ensemble de schémas qui ABANDONNERONT le paquet en cas de correspondance et un autre ensemble de schémas qui ACCEPTERONT le paquet en cas de correspondance.

Commutateur multidestinataire – Un trafic multidestinataire spécifique peut être affecté à son propre réseau local virtuel afin de garantir qu'il n'interfère pas avec le trafic réseau normal et d'assurer une livraison en temps réel grâce à la définition du niveau de priorité requis pour le VLAN désigné. Le commutateur gère l'enregistrement des groupes multidestinataires à l'aide de l'IGMP Snooping et du protocole IGMP.

1.4 Configuration par défaut

TABLEAU 1-2 Configuration par défaut

Fonction	Par défaut
Paramètres système	
Web Mgt. (Gestion Web)	Activée
Secure Web Mgt. (Gestion Web sécurisée)	Désactivée
BOOTP	Activé
DHCP	Activé
SNMP Communities (Communautés SNMP)	publiques : Lecture seule privées : Lecture/Ecriture
SNMP Traps (Interruptions SNMP)	Interruptions d'authentification : activées Evénements de liaison ascendante/descendante : activés
User Name (Nom d'utilisateur)	admin (pour la console, Telnet, Web) guest (pour la console, Telnet, Web)
Password (Mot de passe)	connexion - utilisateur admin, mot de passe « admin » utilisateur guest, mot de passe « guest » Passage de Normal Exec à Privileged Exec : « super »
Serial Port (Port série)	Débit en bauds : 9600, Bits de données : 8, Bits d'arrêt : 1, Parité : aucune
IP Settings (Paramètres IP)	Adresse : 0.0.0.0, Masque de sous-réseau : 255.0.0.0
Port Status (Etat du port)	
Port Speed (Vitesse du port)	Port SNP0-15 : 1000 Mbps Port NETP0-7 : 10/100/1000 Mbps, auto-négocié Port NETMGT : 10/100 Mbps, auto-négocié
Duplex Mode (mode « Duplex »)	Port SNP0-15 : duplex Port NETP0-7, NETMGT : « semi duplex et full duplex », auto-négocié

TABLEAU 1-2 Configuration par défaut

Fonction	Par défaut
Flow Control (Contrôle de flux)	Désactivé
Port Priority (Priorité du port)	Priorité à l'entrée : 0
Port Security (Sécurité du port)	Désactivée
Protocole Spanning Tree	Activé, RSTP par défaut (Valeurs par défaut : tous les paramètres basés sur IEEE 802.1w)
Edge Port (Fast Forwarding) (Port de bord) (Transmission rapide)	Activé par défaut pour SNP0-15, désactivé pour NETP0-7
Address Aging (Obsolescence des adresses)	300 secondes
VLAN (Réseaux locaux virtuels)	
GVRP	Désactivé
Default VLAN (Réseau local virtuel par défaut)	PVID 1 (pour les trames non marquées)
Management VLAN (VLAN de gestion)	VLAN 2 (pour le port de gestion)
Tagging (Marquage)	RX : toutes les trames, TX : trames non marquées
Ingress Filtering (Filtrage à l'entrée)	Désactivé
Multicast Filtering (Filtrage multidestinataire)	
IGMP Snooping	Activé
ARP	Activé
Cache Timeout (Temporisation du cache)	20 minutes

CHAPITRE **2**

Configuration initiale

Pour obtenir des informations complètes sur la configuration initiale du commutateur, reportez-vous au *Manuel d'installation du logiciel du châssis Sun Fire™ B1600 pour serveurs Blade*.

Ce chapitre contient les rubriques suivantes :

2.1 Connexion à l'interface du commutateur

2.1.1 Options de configuration

Le module du commutateur propose une interface de ligne de commande (ILC) de configuration à des fins de gestion. Il est possible d'accéder à ce programme en se connectant au port console série RJ-45 du commutateur, puis en ouvrant l'ILC du commutateur depuis l'invite de commande du contrôleur système, comme indiqué dans les instructions ci-dessous, où SSC*n* indique soit SSC0 soit SSC1.

```
sc>: console sscn/swt
Username: admin
Password:

      CLI session with the Sun Fire B1600 is opened.
      To end the CLI session, enter [Exit].

Console#
```

Remarque - Vous pouvez utiliser une connexion Telnet ou Web au commutateur pour autant que vous ayez configuré un serveur DHCP sur votre réseau de gestion. Pour vous assurer que le commutateur reçoit la même adresse à chaque initialisation (et envoie une requête DHCP), vous devez spécifier l'identificateur de client sur votre serveur DHCP : SUNW,SWITCH_ID=*numéro de série du châssis*, 0 (pour le commutateur en SSC0) ou SUNW,SWITCH_ID=*numéro de série du châssis*, 1 (pour le commutateur en SSC1). Pour obtenir des informations sur la préparation du réseau dans le but de lui adjoindre le châssis du système et sur toutes les procédures visant à configurer le commutateur pour la première fois, reportez-vous au *Manuel d'installation du logiciel du châssis Sun Fire™ B1600 pour serveurs Blade*.

2.1.1.1 Configuration du commutateur par le biais des interfaces intégrées

Connexion à la console – Vous pouvez accéder à l'interface de ligne de commande (ILC) du commutateur en entrant la commande « console ssc*n*/swt », où « n » désigne le SSC0 ou le SSC1, dans l'invite de commande du contrôleur système.

Connexion Telnet – Vous pouvez vous connecter à l'ILC du commutateur à distance par le biais d'une connexion Telnet au réseau de gestion.

Interface Web – Le commutateur comprend également un agent Web HTTP intégré. Il est possible d'accéder à celui-ci à l'aide d'un navigateur Web standard depuis n'importe quel ordinateur du réseau de gestion.

Logiciel SNMP – L'agent de gestion du commutateur est basé sur le protocole SNMP (Simple Network Management Protocol), dont les versions 1 et 2c sont prises en charge. Il permet de gérer le commutateur depuis n'importe quel système du réseau de gestion à l'aide d'un logiciel de gestion tel que SunNet Manager.

Le programme de configuration du système et l'agent SNMP prennent en charge des fonctions de gestion telles que :

- activation/désactivation des ports ;
- réglage de la vitesse/du mode duplex pour les ports ;
- configuration des paramètres SNMP ;
- ajout de ports aux réseaux locaux virtuels ;
- affichage d'informations système ou de statistiques ;
- configuration du commutateur afin que celui-ci puisse rejoindre un Spanning Tree ;
- téléchargement du microprogramme du système.

2.2 Activation de l'accès SNMP à des fins de gestion

Il est possible de configurer le commutateur afin que celui-ci accepte des commandes de gestion provenant d'applications SNMP (Simple Network Management Protocol, v1 ou v2c) telles que SunNet Manager. Vous pouvez le configurer pour qu'il réponde aux requêtes SNMP et/ou génère des interruptions SNMP.

Lorsque les stations de gestion SNMP envoient des requêtes au commutateur (pour obtenir des informations ou pour définir un paramètre), le commutateur fournit les données requises ou définit le paramètre spécifié. Le commutateur peut également être configuré pour envoyer des informations aux gestionnaires SNMP (sans que ceux-ci les demandent) par le biais de messages d'interruption informant le gestionnaire de certains événements.

2.2.1 Chaînes communautaires

Les chaînes communautaires permettent de déterminer l'accès aux stations SNMP à des fins de gestion ainsi que d'autoriser les stations SNMP à recevoir des messages d'interruption provenant du SSC. C'est pourquoi vous devez affecter des chaînes communautaires aux utilisateurs ou groupes d'utilisateurs spécifiés et définir le niveau d'accès ad hoc.

Les chaînes par défaut sont les suivantes :

- **public** - avec un accès en lecture seule. Les stations de gestion autorisées peuvent uniquement récupérer les objets MIB.
- **private** - avec un accès en lecture/écriture. Les stations de gestion autorisées peuvent récupérer et modifier les objets MIB.

Remarque - Si vous n'avez pas l'intention d'utiliser le protocole SNMP, nous vous conseillons d'effacer les deux chaînes communautaires par défaut. S'il n'existe aucune chaîne communautaire, la gestion par le biais d'un accès SNMP au commutateur est désactivée.

Pour configurer une chaîne communautaire, procédez comme suit :

1. Depuis l'invite du mode de configuration globale du niveau d'accès Privileged Exec, entrez « snmp-server community *string mode* », où « string » représente la chaîne d'accès et « mode » signifie **rw** (lecture/écriture) ou **ro** (lecture seule). Appuyez sur <Entrée>.

2. Pour supprimer une chaîne existante, il vous suffit d'entrer « no snmp-server community *string* », où « string » représente la chaîne d'accès à supprimer. Appuyez sur <Entrée>.

```
Console(config)#snmp-server community sun rw
Console(config)#no snmp-server community private
Console(config)#
```

2.2.2 Récepteurs d'interruptions

Vous pouvez également spécifier les stations SNMP qui doivent recevoir des interruptions depuis le SSC.

Pour configurer un récepteur d'interruptions, procédez comme suit :

1. **Depuis l'invite du mode de configuration globale, entrez « snmp-server host *host-address community-string* », où « host-address » représente l'adresse IP du récepteur d'interruptions et « community-string » la chaîne associée à cet hôte.**

   Appuyez sur <Entrée>.

2. **Pour pouvoir configurer le SSC afin qu'il envoie des notifications SNMP, vous devez entrer au moins une commande snmp-server enable traps.**

   Entrez « snmp-server enable traps [*type*] », où « type » est une authentification ou une liaison ascendante-descendante. Appuyez sur <Entrée>.

```
Console(config)#snmp-server enable traps link-up-down
Console(config)#
```

3. **Enregistrez les paramètres de configuration en suivant les instructions figurant dans le** *Manuel d'installation du logiciel du châssis Sun Fire™ B1600 pour serveurs Blade***.**

PART II Configuration du commutateur

Cette section décrit les fonctions de base du commutateur et présente quelques exemples relatifs à la configuration de chacune d'entre elles par le biais d'un navigateur Web ou de l'interface de ligne de commande.

Présentation des opérations de gestion

Référence de la ligne de commande

CHAPITRE **3**

Présentation des opérations de gestion

Le présent chapitre explique comment s'acquitter des tâches de configuration de base.

3.1 Utilisation de l'interface Web

Ce commutateur propose un agent Web HTTP intégré. Celui-ci vous permet de configurer le commutateur et consulter les statistiques afin de contrôler l'activité du réseau, le tout à l'aide d'un navigateur Web. Il est possible d'accéder à l'agent Web à l'aide d'un navigateur Web standard (Internet Explorer 5.0 ou supérieur ou Netscape Navigator 6.2 ou supérieur) depuis n'importe quel ordinateur du réseau.

Remarque - Vous pouvez également employer l'interface de ligne de commande (ILC) pour gérer le commutateur par le biais d'une connexion série au port console ou via Telnet. Pour plus d'informations sur l'utilisation de l'ILC, consultez le chapitre 4.

Avant d'accéder au commutateur depuis un navigateur Web, veillez à accomplir les tâches suivantes :

1. Configurez une adresse IP, un masque de sous-réseau et une passerelle par défaut valables pour le commutateur à l'aide d'une connexion série hors-bande, du protocole BOOTP ou du protocole DHCP. (Pour plus d'informations sur ces opérations, reportez-vous au *Manuel d'installation du logiciel du châssis Sun Fire™ B1600 pour serveurs Blade*.)

2. Définissez un nom d'utilisateur et un mot de passe à l'aide d'une connexion série hors-bande. L'accès à l'agent Web est déterminé par les mêmes nom d'utilisateur et mot de passe que le programme de configuration intégré. (Pour plus d'informations sur ces opérations, reportez-vous au *Manuel d'installation du logiciel du châssis Sun Fire™ B1600 pour serveurs Blade*.)

Remarque - Si le chemin entre votre station de gestion et ce commutateur ne passe pas par un périphérique utilisant l'algorithme Spanning Tree, vous pouvez paramétrer le port du commutateur relié à votre station de gestion pour qu'il utilise la transmission rapide et ce, dans le but d'améliorer les temps de réponse du commutateur aux commandes de gestion émises par le biais de l'interface Web. Voir « Administration du port de périphérie » à la page 4-107.)

---

3. Une fois le nom d'utilisateur et le mot de passe saisis, vous pouvez accéder au programme de configuration du système.

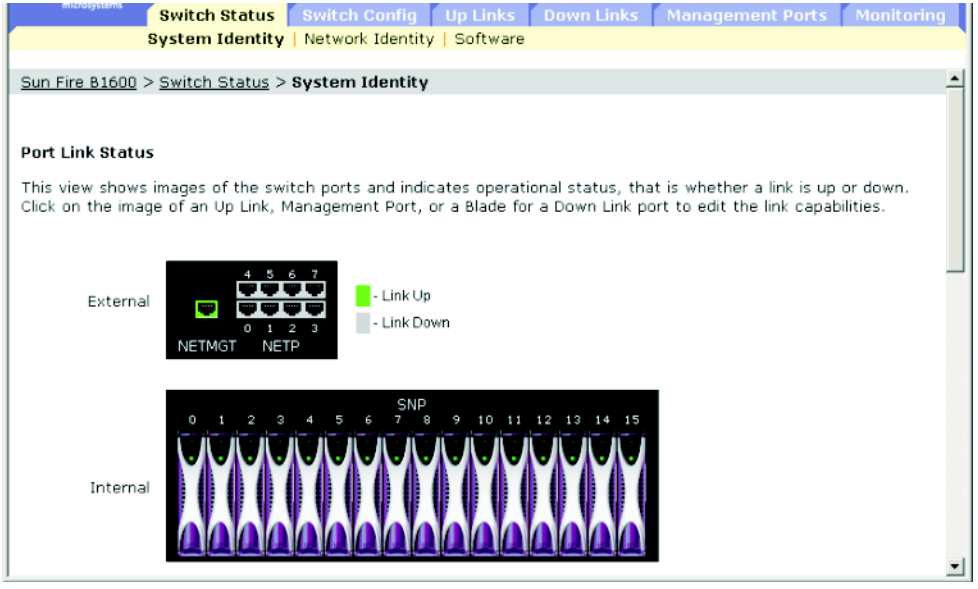
Remarque - Vous avez droit à trois tentatives pour la saisie du mot de passe. Au troisième échec, vous êtes déconnecté.

3.1.1 Navigation dans l'interface du navigateur Web

Pour accéder à l'interface du navigateur Web, vous devez d'abord entrer un nom d'utilisateur et un mot de passe. L'administrateur dispose d'un accès en lecture/écriture à tous les paramètres de configuration et statistiques. Ses nom d'utilisateur et mot de passe par défaut sont « admin ».

3.1.1.1 Page d'accueil

Lorsque votre navigateur Web se connecte à l'agent Web du commutateur, la page d'accueil apparaît. Sélectionnez « Switch » dans le panneau du menu principal situé à gauche de la page. Les options de configuration apparaissent dans les onglets des menus et dans les éléments de menu correspondants (figurant dans la ligne située sous les onglets) présentés en haut de l'écran. Les onglets des menus et les éléments subordonnés servent à accéder aux menus de configuration et à consulter les paramètres de configuration et les statistiques.



3.1.1.2 Options de configuration

Les paramètres configurables proposent une boîte de dialogue ou une liste déroulante. Si vous modifiez la configuration sur une page, veillez à cliquer sur le bouton « Save » afin de valider le nouveau paramètre. Le tableau suivant présente les boutons de configuration affichés sur la page Web.

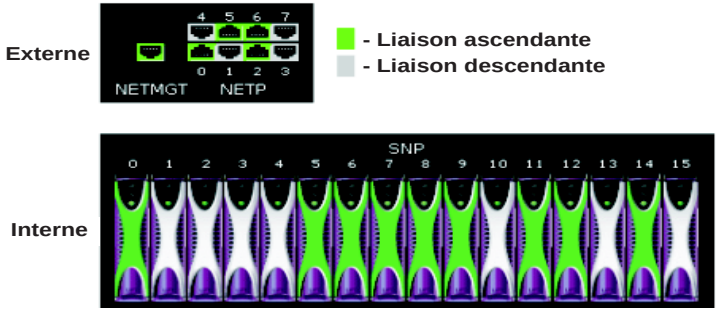
Bouton	Action
Cancel	Annule les valeurs spécifiées et restaure les valeurs courantes.
Reset	Annule les valeurs spécifiées et restaure les valeurs courantes.
Save	Applique les valeurs spécifiées au système.

Remarque - Pour vous assurer que l'écran s'actualise correctement, vérifiez qu'Internet Explorer 5.x est configuré comme suit : sous le menu « Outils / Options Internet / Général / Fichiers Internet temporaires / Paramètres », la valeur de l'élément « Vérifier s'il existe une version plus récente des pages enregistrées » doit être « A chaque visite de la page ».

Remarque - Si vous utilisez Internet Explorer 5.0, il est possible que vous deviez actualiser l'écran manuellement après avoir apporté des modifications à la configuration. Pour ce faire, appuyez sur le bouton « Actualiser » de votre navigateur.

3.1.2 Affichage du tableau de bord

L'agent Web affiche une image des ports à liaison ascendante du commutateur indiquant si chaque liaison s'effectue de manière ascendante ou descendante. Cliquez sur l'image d'un port pour ouvrir la page de configuration correspondante, conformément à la description de la page 4-80.



3.1.3 Menu principal

A l'aide de l'agent Web intégré, vous pouvez définir les paramètres système, gérer et contrôler le commutateur et tous ses ports ou encore surveiller l'état du réseau. La table suivante décrit brièvement les sélections disponibles depuis ce programme.

Menu	Description	Page
Switch Setup	Configuration de base	4-8
System Identity	Propose une description de base du système, y compris son emplacement et ses informations de contact	4-8
Network Identity	Définit l'adresse IP pour un accès à des fins de gestion, via DHCP, BOOTP ou une configuration manuelle	4-11
Software	Affiche la version du microprogramme, télécharge le code et les paramètres de configuration.	4-17
Switch Config	Protocoles de configuration globale	4-34
Security	Affecte des noms d'utilisateur et des mots de passe, de même qu'un service d'authentification pour l'accès à distance via RADIUS ou TACACS+	4-24
Communication	Définit les chaînes de communauté SNMP, les gestionnaires d'interruptions ainsi que le type d'interruptions à émettre	4-30
VLAN	Affiche des informations de base sur les VLAN ; active le protocole multidestinataire GVRP ; configure les VLAN	4-34
Static VLAN Port Membership	Ajoute des membres statiques aux VLAN	4-42
Broadcast & Multicast	Définit le contrôle des orages de diffusion ; configure les protocoles multidestinataires, y compris l'IGMP Snooping, les informations sur le port de routage statique et les services multidestinataires	4-45
IGMP Parameters	Active le filtrage multidestinataire ; configure les paramètres des requêtes multidestinataires	4-46
Multicast Router Ports	Affecte les ports reliés à un commutateur/routeur multidestinataire avoisinant	4-49
Multicast Services	Affecte un service multidestinataire à une interface spécifique	4-52
Broadcast Parameters	Définit le seuil des orages de diffusion	4-55
Spanning Tree	Configure le protocole Spanning Tree	4-57
Basic Configuration	Configure les paramètres du Spanning Tree global	4-57
Advanced Configuration	Configure les paramètres avancés du RSTP	4-63

Menu	Description	Page
Class of Service	Configure la classe de service	4-65
Basic Traffic Prioritisation	Configure les priorités CdS par défaut, établit des correspondances entre ces priorités et les files d'attente de sortie et configure la mise en file d'attente WRR (Weighted Round Robin)	4-65
Layer 3/4 Traffic Prioritisation	Sélectionne le service de priorité de la couche 3/4, établit des correspondances entre les marques de priorité et les valeurs CdS et entre les marques DSCP et les valeurs CdS.	4-71
Address Tables	Définit l'obsolescence des adresses, affiche les entrées relatives à l'interface, l'adresse ou le VLAN spécifiés ; configure les adresses statiques	4-77
Up Links	Configuration du port	4-80
Connection Status	Affiche l'état de connexion du port	4-80
Connection Configuration	Configure les paramètres de connexion du port ; active le contrôle des orages de diffusion	4-84
Link Aggregation	Configure les ports à regrouper de manière dynamique à l'aide du protocole LACP ou spécifie des ports à regrouper de manière statique	4-88
VLAN	Spécifie les attributs des ports (y compris le PVID par défaut, le mode « switchport », le filtrage à l'entrée, le GVRP, les horloges GARP) ; configure les membres statiques des VLAN	4-93
Static Addresses	Affiche ou édite les entrées statiques de la table d'adressage ; active/désactive l'apprentissage des entrées permanentes	4-100
Spanning Tree	Configure les paramètres de port du Spanning Tree global	4-103
Spanning Tree Protocol	Configure les paramètres STA au niveau du port pour l'interface (les interfaces) du Spanning Tree global	4-103
Down Links	Configuration du port	4-80
Connection Status	Affiche l'état de connexion du port	4-80
Connection Configuration	Configure les paramètres de connexion du port ; active le contrôle des orages de diffusion	4-84
Link Aggregation	Configure les ports à regrouper de manière dynamique à l'aide du protocole LACP ou spécifie des ports à regrouper de manière statique	4-88
VLAN	Spécifie les attributs des ports (y compris le PVID par défaut, le mode « switchport », le filtrage à l'entrée, le GVRP, les horloges GARP) ; configure les membres statiques des VLAN	4-93

Menu	Description	Page
Static Addresses	Affiche ou édite les entrées statiques de la table d'adressage ; active/désactive l'apprentissage des entrées permanentes	4-100
Spanning Tree	Configure les paramètres de port du Spanning Tree global	4-103
Spanning Tree Protocol	Configure les paramètres STA au niveau du port pour l'interface du Spanning Tree global	4-103
Management Port	Configuration du port	4-80
Connection Status	Affiche l'état de connexion du port	4-80
VLAN	Spécifie les attributs des ports (y compris le PVID par défaut, le mode « switchport », le filtrage à l'entrée, le GVRP, les horloges GARP) ; configure les membres statiques des VLAN	4-93
Packet Filtering	Filtre le trafic entrant dans le port de gestion depuis les ports à liaison ascendante	4-111
Monitoring	Fonctions de contrôle du commutateur	4-116
Port Mirroring	Définit les ports source et cible pour la mise en miroir	4-116
Port Statistics	Affiche les statistiques relatives au trafic du port, y compris les informations provenant du groupe d'interfaces, de la base d'informations de gestion (MIB) Ethernetlike et de la base d'informations de gestion (MIB) RMON	4-118
SNMP Statistics	Affiche les statistiques relatives aux messages SNMP	4-127
Logs	Configure les paramètres des journaux ; affiche les messages enregistrés dans la mémoire du commutateur	4-127

3.2 Configuration de base

3.2.1 Affichage des informations relatives au système

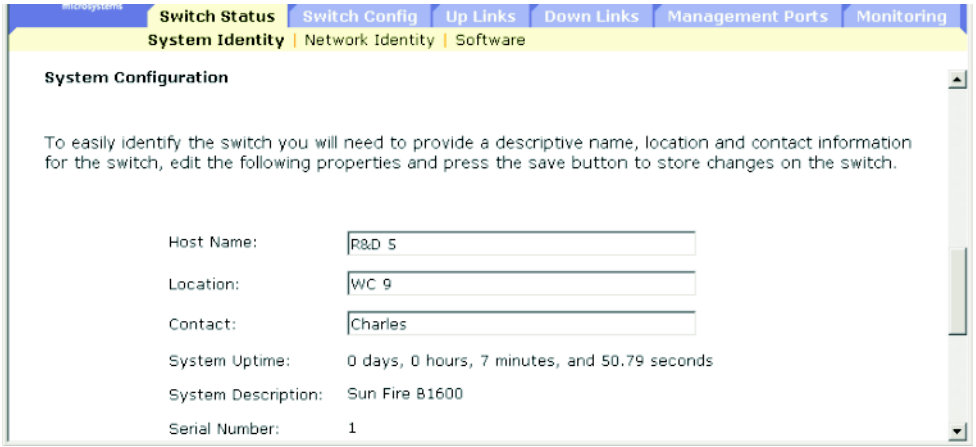
Pour identifier le système aisément, donnez-lui un nom descriptif, un emplacement et des informations de contact.

Attributs des commandes

- **Host Name** : Nom attribué au commutateur.
- **Location** : Emplacement du châssis.
- **Contact** : Administrateur responsable du système.
- **System Up Time** : Délai pendant lequel l'agent de gestion a fonctionné.
- **System Description** : Description du matériel du système affecté par le fabricant.
- **Serial Number**[1] : Numéro de série de la carte mère.
- **System OID string**[2] **:** Identificateur de l'objet MIB II pour le sous-système de gestion du réseau du commutateur.
- **MAC Address**[3] : Adresse de ce commutateur sur la couche physique.
- **Web server**[2] : Indication de l'activation/désactivation de l'accès à la gestion via HTTP.
- **Web server port**[2] : Indication du numéro de port TCP utilisé par l'interface Web.
- **POST result**[2] : Affichage des résultats du test à la mise sous tension.

1: ILC : Reportez-vous à la section « show version » à la page 4-40
2: ILC uniquement
3: Web : voir « Définition de l'adresse IP » à la page 3-11.

Web : Ouvrez Switch Setup (Configuration du commutateur)=>System Identity (Identité système). Indiquez le nom de l'hôte, l'emplacement et les informations de contact de l'administrateur système, puis cliquez sur « Save Changes ».



ILC : Indiquez le nom de l'hôte, son emplacement ainsi que ses informations de contact.

```
Console(config)#hostname R&D 5                                    4-25
Console(config)#snmp-server location WC 9                         4-50
Console(config)#snmp-server contact Bill                          4-49
Console#show system4-38
System description: Sun Fire B1600
System OID string: 1.3.6.1.4.1.674.10895.4
System information
 System Up time: 0 days, 0 hours, 55 minutes, and 54.91 seconds
 System Name            : [NONE]
 System Location        : [NONE]
 System Contact         : [NONE]
 MAC address            : 00-00-e8-00-00-01
 Web server             : enable
 Web server port        : 80
 Web secure server      : enable
 Web secure server port : 443
 POST result

--- Performing Power-On Self Tests (POST) ---
UART Loopback Test ..................... PASS
Timer Test ............................. PASS
DRAM Test .............................. PASS
I2C Initialization ..................... PASS
Runtime Image Check .................... PASS
PCI Device Check ....................... PASS
Switch Driver Initialization ........... PASS
------------------- DONE --------------------
Console#
```

SNMP : Variables MIB équivalentes.

Nom de zone	Variable MIB	Accès	Plage de valeurs	Valeur par défaut
System Name (Host Name)	MIB-II. system. sysName	Lecture/ Ecriture	Chaîne (Taille (0-255))	
System Location	MIB-II. system. sysLocation	Lecture/ Ecriture	Chaîne (Taille (0-255))	
System Contact	MIB-II. system. sysContact	Lecture/ Ecriture	Chaîne (Taille (0-255))	
System Up Time	MIB-II. system. sysUpTime	Lecture seule	Temps (en centisecondes)	
System Description	MIB-II. system. sysDescr	Lecture seule	Chaîne (Taille (0-255))	
System Object Identification	MIB-II. system. sysObjectID	Lecture seule	Identificateur de l'objet	
MAC Address	MIB-II. interfaces. ifTable.ifEntry. ifPhysAddress	Lecture seule	Adresse physique	
HTTP State (Web Server)	sun... ipMgt. ipHttpState	Lecture/ Ecriture	enabled (activé) (1), disabled (désactivé) (2)	enabled
HTTP Port (Web Server Port)	sun... ipMgt. ipHttpPort	Lecture/ Ecriture	Nombre entier (1-65535)	80
HTTPS State (Secure Server)	sun... ipMgt. ipHttpsState	Lecture/ Ecriture	enabled (activé) (1), disabled (désactivé) (2)	enabled
HTTPS Port (Secure Server Port)	sun... ipMgt. ipHttpsPort	Lecture/ Ecriture	Nombre entier (1-65535)	443

3.2.2 Définition de l'adresse IP

Par défaut, le commutateur recherche son adresse IP, sa passerelle par défaut et son masque de sous-réseau à l'aide de DHCP.

Vous pouvez configurer manuellement une adresse IP spécifique ou ordonner au périphérique d'obtenir une adresse par le biais d'un serveur DHCP ou BOOTP. Les adresses IP valables se composent de quatre nombres décimaux, de 0 à 255, séparés par des points. Aucun autre format n'est accepté par le logiciel.

Remarque - L'adresse IP du commutateur est en fait l'adresse IP du VLAN contenant le port de gestion (NETMGT). Par défaut, le port de gestion se trouve sur le VLAN 2. Par conséquent, c'est en affectant une adresse IP au VLAN 2 que vous configurez un accès réseau au commutateur. Seul le VLAN contenant le port de gestion doit se voir affecter une adresse IP. Lorsque vous affectez une adresse IP à un VLAN quelconque, l'adresse IP originale est immédiatement désactivée, et la nouvelle adresse prend effet simultanément.

Attributs des commandes

- **Current IP Address** : Adresse courante de l'interface VLAN disposant de droits de gestion.
- **MAC Address**[1] : Adresse de ce commutateur sur la couche physique.
- **Management VLAN** : Il s'agit du seul VLAN vous permettant de gérer le commutateur. Par défaut, le port de gestion (NETMGT) est configuré comme membre de ce VLAN (à savoir VLAN 2). Toutefois, si vous modifiez le VLAN de gestion, vous ne pouvez plus gérer le commutateur, à moins que le port NETMGT ait déjà été configuré comme membre du nouveau VLAN. Dans ce cas, vous devez utiliser l'interface de la console pour ajouter le port NETMGT au nouveau VLAN de gestion configuré. Reportez-vous à la « switchport allowed vlan » à la page 4-112.

1: ILC : voir « Affichage des informations relatives au système » à la page 3-8.

- **IP Address Mode** : Spécifie si la fonctionnalité IP est activée par le biais d'une configuration manuelle (statique), d'un protocole DHCP (Dynamic Host Configuration Protocol) ou d'un protocole BOOTP (Boot Protocol). Si les protocoles DHCP/BOOTP sont activés, le protocole IP ne fonctionne que lorsqu'une réponse du serveur est reçue. Des requêtes sont diffusées périodiquement par le commutateur pour les paramètres de configuration IP. (Les valeurs DHCP/BOOTP peuvent inclure l'adresse IP, le masque de sous-réseau et la passerelle par défaut.)
  - **DHCP** : Dynamic Host Configuration Protocol
    - **Enable Client ID** : Inclut un identificateur client dans toutes les communications avec le serveur DHCP.
      - **Text / Hex** : Indique si l'identificateur du client a été entré sous la forme d'une chaîne de texte (1-15 caractères) ou d'une valeur hexadécimale. Le type de données utilisé dépend des exigences de votre serveur DHCP.

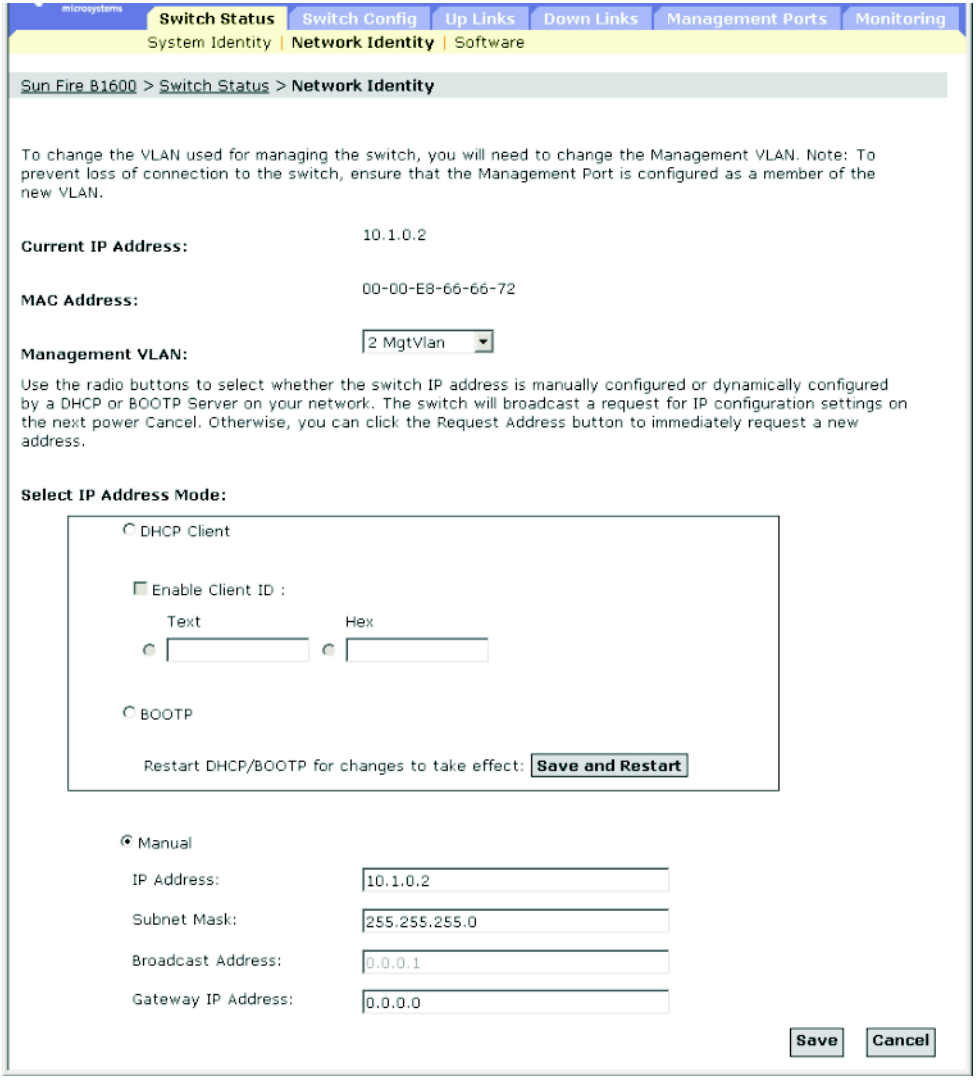
Remarque - L'identificateur client spécifié dans ce menu sera écrasé par le contrôleur système lors du prochain réamorçage du système ou du commutateur. La zone Client ID sera supprimée de la prochaine version du microprogramme.

  - **BOOTP** : Boot Protocol
- **Manual** : Définit des valeurs spécifiques pour l'interface de gestion.
  - **IP Address** : Adresse de l'interface VLAN autorisant la gestion. Les adresses IP valables se composent de quatre nombres, de 0 à 255, séparés par des points. (Par défaut : 0.0.0.0)
  - **Subnet Mask** : Ce masque identifie l'adresse de l'hôte utilisée pour le routage vers des sous-réseaux spécifiques. (Par défaut : 255.0.0.0)
  - **Broadcast Address**[2] : Adresse de diffusion IP utilisée pour envoyer des datagrammes sur l'interface associée à l'adresse IP. Cette valeur s'applique tant aux adresses de sous-réseau qu'aux adresses de diffusion réseau utilisées par le commutateur. (Par défaut : 0.0.0.1)
  - **Gateway IP Address** : Adresse IP du routeur de passerelle entre ce périphérique et les stations de gestion existant sur les autres segments du réseau. (Par défaut : 0.0.0.0)

2: Web uniquement

3.2.2.1 Configuration manuelle

Web : Ouvrez Switch Setup=>Network Identity. Sélectionnez l'interface de gestion, cliquez sur la case d'option Manual, spécifiez l'adresse IP, le masque de sous-réseau et la passerelle par défaut, puis cliquez sur Save.



Remarque - Si vous recevez un message d'erreur vous indiquant que les données saisies ne sont pas valables, vérifiez chacune des adresses IP spécifiées.

ILC : Spécifiez l'interface de gestion, l'adresse IP et la passerelle par défaut.

```
Console#config
Console(config)#interface vlan 2 4-74
Console(config-if)#ip address 10.1.0.2 255.255.255.0          4-62
Console(config-if)#exit
Console(config)#ip default-gateway 10.1.0.254 4-65
Console(config)#
```

SNMP : Variables MIB équivalentes.

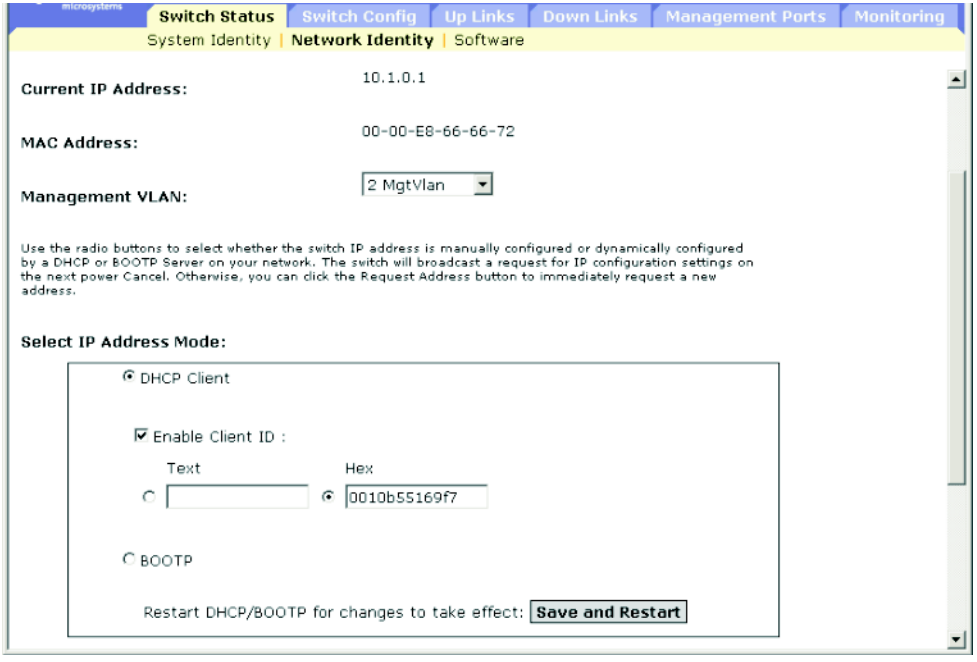
Nom de zone	Variable MIB	Accès	Plage de valeurs	Valeur par défaut
Management VLAN	sun... switchMgt. switchManagementVlan	Lecture/ Ecriture	Nombre entier (1-4094)	1
IP Address Mode	sun... vlanMgt. vlanTable.vlanEntry. vlanAddressMethod	Lecture/ Ecriture	user (1), bootp (2), dhcp (3)	user
IP Address Configuration	MIB-II. ip.ipAddrTable. ipAddrEntry. ipAdEntAddr	Lecture/ Ecriture	Adresse IP	
Subnet Mask Configuration	MIB-II. ip.ipAddrTable. ipAddrEntry. ipAdEntNetMask	Lecture/ Ecriture	Adresse IP	
Broadcast Address	MIB-II. ip.ipAddrTable. ipAddrEntry. ipAdEntBcastAddr	Lecture seule	Nombre entier (0-1)	1
Default Gateway Configuration	sun... ipMgt. netDefaultGateway	Lecture/ Ecriture	Adresse IP	

3.2.2.2 Utilisation des protocoles DHCP/BOOTP

Par défaut, le commutateur utilise les services DHCP/BOOTP pour rechercher les informations relatives à sa configuration IP.

Web : Ouvrez Switch Setup (Configuration du commutateur)=>Network Identity (Identité réseau). Spécifiez l'interface de gestion et cliquez sur la case d'option DHCP ou BOOTP.

Par défaut, le contrôleur système du châssis fournit un identificateur client au commutateur. Il s'agit de SUNW,SWITCH_ID=*numéro de série du châssis*,0 ou de SUNW,SWITCH_ID=*numéro de série du châssis*,1 (selon que le commutateur se trouve en SSC0 ou en SSC1). Vous pouvez spécifier un identificateur client dans la case à cocher Enable Client ID, mais il sera écrasé lorsque le contrôleur système sera réinitialisé ou réamorcé. Nous vous déconseillons donc de le faire. La zone Enable Client ID disparaîtra des versions ultérieures du microprogramme.



Remarque - Si vous perdez votre connexion de gestion, utilisez une connexion console et entrez « show ip interface » pour déterminer la nouvelle adresse du commutateur.

Remarque - L'identificateur client spécifié dans ce menu sera écrasé par le contrôleur système lors du prochain réamorçage du contrôleur système ou du commutateur. La zone Client ID sera supprimée de la prochaine version du microprogramme.

ILC : Spécifiez l'interface de gestion, configurez le mode de l'adresse IP sur DHCP ou BOOTP, puis entrez la commande « ip dhcp restart ».

```
Console#config
Console(config)#interface vlan 2 4-74
Console(config-if)#ip address dhcp 4-62
Console(config-if)#ip dhcp client-id hex 00-00-e8-66-65-72 4-64
Console(config-if)#end
Console#ip dhcp restart                                          4-64
Console#show ip interface                                        4-66
IP address and netmask: 10.1.0.54 255.255.255.0 on VLAN 2,
 and address mode: DHCP.
Console#
```

Renewing DCHP : DHCP peut attribuer des adresses aux clients pour une durée indéterminée ou pour une période spécifique. Si l'adresse expire ou si le commutateur passe à un autre segment du réseau, vous ne pouvez plus gérer le commutateur. Dans ce cas, vous pouvez réamorcer le commutateur ou soumettre une requête client pour redémarrer le service DHCP.

Web : Si l'adresse affectée par DHCP ne fonctionne plus, vous ne pouvez pas renouveler les paramètres IP via l'interface Web. Vous ne pouvez redémarrer le service DHCP depuis l'interface Web que si l'adresse courante est toujours valable.

ILC : Entrez la commande suivante pour redémarrer le service DHCP.

```
Console#ip dhcp restart 4-64
```

SNMP : Variables MIB équivalentes.

Nom de zone	Variable MIB	Accès	Plage de valeurs	Valeur par défaut
Management VLAN	sun... switchMgt. switchManagementVlan	Lecture/ Ecriture	Nombre entier (1-4094)	1
IP Address Mode	sun... vlanMgt. vlanTable.vlanEntry. vlanAddressMethod	Lecture/ Ecriture	user (1), bootp (2), dhcp (3)	dchp
DHCP Client ID	sun... ipMgt. dhcpClientIfClientId	Lecture/ Ecriture	Chaîne d'octets (Adresse MAC)	
DHCP Restart	sun... ipMgt. ipDhcpRestart	Lecture/ Ecriture	restart (1), noRestart (2)	noRestart

3.2.3 Affichage des versions logicielles du commutateur

Attributs des commandes

- **Loader Version** : Numéro de version du code de chargement.
- **Boot-ROM Version** : Numéro de version du code d'amorce.
- **Operation Code Version** : Numéro de version du code runtime.
- **Unit ID*** **:** Identificateur du commutateur actif. (Cette valeur est toujours de 1.)

* ILC uniquement. La valeur de l'identificateur d'unité ne joue aucun rôle dans la version courante du commutateur dans le châssis B1600 du serveur Blade Stiletto.

Web : Ouvrez Switch Setup=>Software.

ILC : Utilisez la commande suivante pour afficher les informations de version.

```
Console#show version                                          4-40
Unit1
 Serial number          :1
 Service tag            :
 Hardware version       :R0B
 Number of ports        :25
 Main power status      :up
 Redundant power status :not present
Agent(master)
 Unit id                :1
 Loader version         :0.0.6.5
 Boot rom version       :0.0.7.3
 Operation code version :1.0.0.1
Console#
```

SNMP : Variables MIB équivalentes.

Nom de zone	Variable MIB	Accès	Plage de valeurs	Valeur par défaut
Switch Serial Number	SUN. switchMgt. switchInfoTable. switchInfoEntry. swSerialNumber	Lecture seule	Chaîne d'affichage (Taille (0..80))	
Switch Hardware Version	SUN. switchMgt. switchInfoTable. switchInfoEntry. swHardwareVer	Lecture seule	Chaîne d'affichage (Taille (0..20))	
Switch Port Number	SUN. switchMgt. switchInfoTable. switchInfoEntry. swPortNumber	Lecture seule	Nombre entier	25
Switch Unit Index	SUN. switchMgt. switchInfoTable. switchInfoEntry. swUnitIndex	Non accessible	Nombre entier	1
Switch Loader Version	sun... switchMgt. switchInfoTable. switchInfoEntry. swLoaderVer	Lecture seule	Chaîne (Taille (0-20))	
Switch Boot Rom Version	sun... switchMgt. switchInfoTable. switchInfoEntry. swBootRomVer	Lecture seule	Chaîne (Taille (0-20))	
Switch Operation Code Version	sun... switchMgt. switchInfoTable. switchInfoEntry. swOpCodeVer	Lecture seule	Chaîne (Taille (0-20))	

3.2.4 Gestion du microprogramme

Vous pouvez charger/télécharger le microprogramme vers/depuis un serveur TFTP. Si vous enregistrez le code runtime dans un fichier sur un serveur TFTP, ce fichier peut ultérieurement être téléchargé sur le commutateur afin de restaurer celui-ci. Vous pouvez également configurer le commutateur afin que celui-ci utilise le nouveau microprogramme sans écraser la version antérieure.

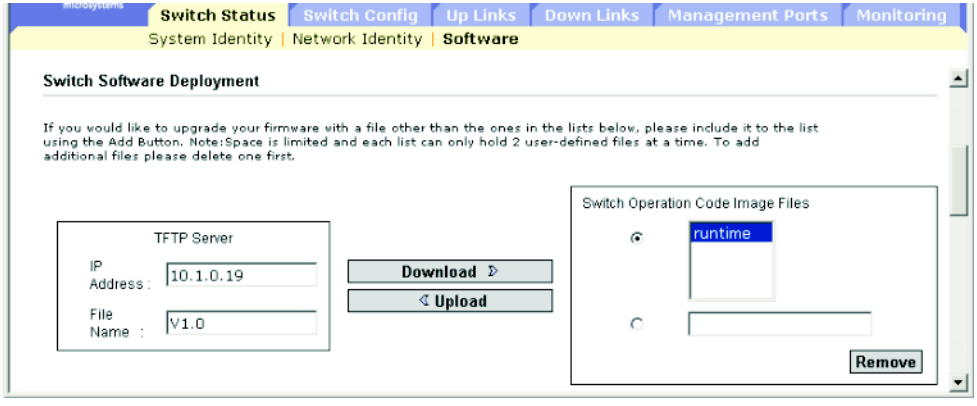
Attributs des commandes

- Le nom du fichier de destination ne doit pas contenir de barres obliques (\ ou /), il ne doit pas commencer par un point (.) et, sur un serveur TFTP, sa longueur maximale ne peut pas dépasser 127 caractères ou 32 caractères pour les fichiers du commutateur. (Caractères valables : A-Z, a-z, 0-9, « . », « - », « _ »)
- Seules deux copies du fichier du logiciel système (contenant le microprogramme runtime) peuvent être enregistrées dans le répertoire de fichiers du commutateur. La version de démarrage courante de ce fichier ne peut pas être supprimée. Si vous enregistrez deux copies du fichier du logiciel système, vous pouvez supprimer celle qui n'est pas actuellement désignée comme version de démarrage et la remplacer par un nouveau fichier, ou vous pouvez copier un nouveau fichier dans le répertoire en utilisant l'un des noms de fichiers existants. Il est également possible de supprimer la désignation comme fichier de démarrage du fichier courant, le supprimer, copier une nouvelle version du fichier du logiciel système dans le répertoire, puis le désigner comme fichier de démarrage.

3.2.4.1 Téléchargement du logiciel système depuis un serveur

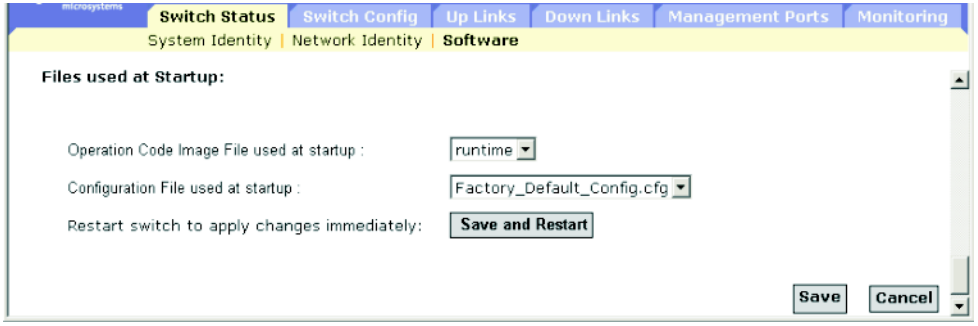
Lorsque vous téléchargez un code runtime, vous pouvez spécifier le nom du fichier de destination pour remplacer l'image courante ou d'abord télécharger le fichier à l'aide d'un nom différent du fichier courant, puis configurer le nouveau fichier comme fichier de démarrage.

Web : Ouvrez Switch Status=>Software. Entrez l'adresse IP du serveur TFTP, entrez le nom du fichier du logiciel à télécharger, sélectionnez un fichier du commutateur à écraser ou spécifiez un nouveau nom de fichier, puis cliquez sur Download.



Remarque - Si vous recevez un message d'erreur indiquant que les données saisies ne sont pas valables, il est possible que vous ayez entré une adresse IP ou un nom de fichier erronés, ou encore que vous ne disposiez pas des droits d'accès requis pour le transfert TFTP. Il est également possible que l'espace mémoire disponible sur le commutateur ne soit pas suffisant.

Si vous téléchargez les données dans un nouveau fichier de destination, sélectionnez celui-ci dans la zone de liste déroulante du code de fonctionnement utilisé au démarrage, puis cliquez sur Save. Pour démarrer le nouveau microprogramme, réamorcez le système en cliquant sur Save et Restart.



ILC : Entrez l'adresse IP du serveur TFTP, sélectionnez le type de fichier config ou opcode, puis entrez les noms des fichiers source et cible, configurez le nouveau fichier afin qu'il démarre le système, puis redémarrez le commutateur.

```
Console#copy tftp file4-18
TFTP server ip address: 10.1.0.99
Choose file type:
 1. config:  2. opcode: <1-2>: 2
Source file name: v10.bix
Destination file name: V10000
\Write to FLASH Programming.
-Write to FLASH finish.
Success.

Console#config
Console(config)#boot system opcode: V100004-23
Console(config)#exit
Console#reload4-16
```

Pour démarrer le nouveau microprogramme, vous devez entrer la commande « reload » afin de réamorcer le système.

SNMP : Variables MIB équivalentes.

Nom de zone	Variable MIB	Accès	Plage de valeurs
Switch Operation Code Image Files	*Non défini*		
TFTP Server IP Address	sun... tftpMgt. tftpServer	Lecture/ Ecriture	Adresse IP
TFTP File Type	sun... tftpMgt. tftpFileType	Lecture/ Ecriture	opcode (1), config (2)
TFTP Source File Name	sun... tftpMgt. tftpSrcFile	Lecture/ Ecriture	Chaîne (Taille (0-127))
TFTP Destination File Name	sun... tftpMgt. tftpDestFile	Lecture/ Ecriture	Chaîne (Taille (0-127))
TFTP Action	sun... tftpMgt. tftpAction	Lecture/ Ecriture	notDownloading (1), downloadToPROM (2), downloadToRAM (3) (*non pris en charge)* upload (4)
TFTP Status	sun... tftpMgt. tftpStatus	Lecture/ Ecriture	tftpSuccess (1), tftpStatusUnknown (2), tftpGeneralError (3), tftpNoResponseFromServer (4), tftpDownloadChecksumError (5), tftpDownloadIncompatible Image(6), tftpTftpFileNotFound(7), tftpTftpAccessViolation(8)
Restart Operation Code File	sun... restartMgt. restartOpCodeFile	Lecture/ Ecriture	Chaîne d'affichage (Taille (0-127))
Restart Action	sun... restartMgt. restartControl	Lecture/ Ecriture	running (1), warmBoot (2), coldBoot (3)

3.2.5 Enregistrement ou restauration des paramètres de configuration

Vous pouvez charger/télécharger les paramètres de configuration vers/depuis un serveur TFTP. Le fichier de configuration peut être téléchargé ultérieurement afin de restaurer les paramètres du commutateur.

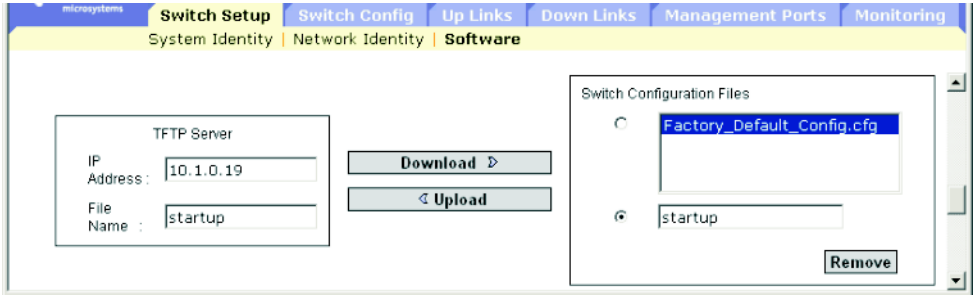
Attributs des commandes

- Le nom du fichier de destination ne doit pas contenir de barres obliques (\ ou /), il ne doit pas commencer par un point (.) et, sur un serveur TFTP, sa longueur maximale ne peut pas dépasser 127 caractères ou 32 caractères pour les fichiers du commutateur. (Caractères valables : A-Z, a-z, 0-9, « . », « - », « _ »)
- Le nombre maximal de fichiers de configuration définis par l'utilisateur dépend de la mémoire disponible.

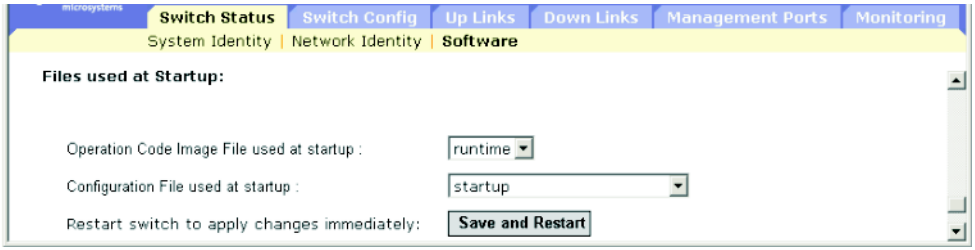
3.2.5.1 Téléchargement des paramètres de configuration depuis un serveur

Vous pouvez télécharger le fichier de configuration sous un nouveau nom de fichier, puis le définir comme fichier de démarrage, ou vous pouvez spécifier le fichier de configuration du démarrage courant comme fichier de destination afin de le remplacer directement. Remarquez que « Factory_Default_Config.cfg » peut être copié sur le serveur TFTP, mais ne peut pas être utilisé comme destination sur le commutateur.

Web : Ouvrez Switch Setup=>Software. Entrez l'adresse IP du serveur TFTP, entrez le nom du fichier à télécharger, sélectionnez un fichier du commutateur à écraser ou spécifiez un nouveau nom de fichier, puis cliquez sur Download.



Si vous téléchargez les données dans un fichier portant un nouveau nom, sélectionnez celui-ci dans la zone de liste déroulante, puis cliquez sur Save. Pour utiliser les nouveaux paramètres, réamorcez le système en cliquant sur Save et Restart.



ILC : Entrez l'adresse IP du serveur TFTP, spécifiez le fichier source sur le serveur, définissez le nom du fichier de démarrage sur le commutateur, puis redémarrez le commutateur.

```
Console#copy tftp startup-config4-18
TFTP server ip address: 192.168.1.19
Source configuration file name: startup2.0
Startup configuration file name [startup] : startup2.0
\Write to FLASH Programming.
-Write to FLASH finish.
Success.

Console#reload
System will be restarted, continue <y/n>?y
```

Si vous téléchargez le fichier de configuration du démarrage sous un nouveau nom, vous pouvez définir ce fichier comme fichier de démarrage ultérieurement, puis redémarrer le commutateur.

```
Console#config
Console(config)#boot system config: startup-new4-23
Console(config)#exit
Console#reload                                                    4-16
System will be restarted, continue <y/n>?y
```

SNMP : Variables MIB équivalentes.

Nom de zone	Variable MIB	Accès	Plage de valeurs
TFTP Server IP Address	sun... tftpMgt. tftpServer	Lecture/ Ecriture	Adresse IP
TFTP File Type	sun... tftpMgt. tftpFileType	Lecture/ Ecriture	opcode (1), config (2)

Nom de zone	Variable MIB	Accès	Plage de valeurs
TFTP Source File Name	sun... tftpMgt. tftpSrcFile	Lecture/ Ecriture	Chaîne d'affichage (Taille (0-127))
TFTP Action	sun... tftpMgt. tftpAction	Lecture/ Ecriture	notDownloading (1), downloadToPROM (2), downloadToRAM (3), upload (4)
TFTP Status	sun... tftpMgt. tftpStatus	Lecture/ Ecriture	tftpSuccess (1), tftpStatusUnknown (2), tfttpGeneralError (3), tftpNoResponseFromServer (4), tftpDownloadChecksumError (5), tftpDownloadIncompatibleImage(6), tftpTftpFileNotFound(7), tftpTftpAccessViolation(8)
Restart Configuration File	sun... restartMgt. restartConfigFile	Lecture/ Ecriture	Chaîne d'affichage (Taille (0-127))
Restart Action	sun... restart.Mgt. restartControl	Lecture/ Ecriture	running (1), warmBoot (2), coldBoot (3)

3.2.6 Configuration de l'authentification utilisateur

Le menu Security vous permet de limiter l'accès à des fins de gestion sur la base des noms d'utilisateur et mots de passe spécifiés. Vous pouvez configurer manuellement les droits d'accès sur le commutateur ou utiliser un serveur d'authentification distant sur la base des protocoles RADIUS ou TACACS +.

Il existe deux types de droits d'accès, Normal et Privileged. Le niveau Privileged permet d'accéder à toutes les commandes, alors que le niveau Normal n'active que certaines d'entre elles. Le compte administrateur par défaut dispose d'un accès en écriture pour tous les paramètres régissant l'agent intégré. Par conséquent, nous vous conseillons de lui attribuer un mot de passe dès que possible et de le conserver en lieu sûr.

Remarque - Le nom d'utilisateur par défaut pour l'administrateur est « admin », avec le mot de passe « admin ».

Utilisation de la commande

- Par défaut, les droits de gestion sont toujours vérifiés à l'aide de la base de données d'authentification placée sur le commutateur local. Si vous avez recours à un serveur d'authentification distant, vous devez spécifier la séquence d'authentification et les paramètres correspondants pour chaque protocole d'authentification à distance spécifié.
- Les protocoles RADIUS (Remote Authentication Dial-in User Service) et TACACS (Terminal Access Controller Access Control System) sont des protocoles d'authentification à la connexion utilisant un logiciel tournant sur un serveur central pour contrôler l'accès aux périphériques RADIUS ou TACACS sur le réseau. Un serveur d'authentification contient une base de données comprenant plusieurs paires nom d'utilisateur/mot de passe avec les niveaux de privilèges associés pour chaque utilisateur ou groupe requérant un accès au commutateur dans le but de gérer celui-ci.

Remarque : Lorsque vous définissez des niveaux de privilèges sur un serveur RADIUS ou TACACS, n'oubliez pas que le niveau 0 permet un accès guest (Normal Exec) au commutateur. Seul le niveau 15 permet un accès administrateur (à savoir Privileged Exec).

- RADIUS utilise le protocole UDP alors que TACACS a recours au protocole TCP. Le protocole UDP n'offre qu'une livraison « best effort » alors que le protocole TCP propose un transfert orienté sur la connexion. De même, remarquez que RADIUS ne chiffre le mot de mot de passe que dans le paquet de demande d'accès du client au serveur, alors que TACACS chiffre l'ensemble du paquet.
- L'authentification à la connexion par RADIUS et TACACS détermine les droits de gestion par le biais du port de console, du navigateur Web ou de Telnet. Ces options d'accès doivent être configurées sur le serveur d'authentification.
- L'authentification à la connexion par RADIUS et TACACS affecte un niveau de privilèges spécifique pour chaque paire nom d'utilisateur/mot de passe. Le nom d'utilisateur, le mot de passe et le niveau de privilèges doivent être configurés sur le serveur d'authentification.
- Vous pouvez spécifier entre une et trois méthodes d'authentification pour chaque utilisateur afin d'indiquer la séquence d'authentification. Par exemple, si vous sélectionnez (1) RADIUS et (2) Local, le nom d'utilisateur et le mot de passe du serveur RADIUS sont vérifiés en premier lieu. Si le serveur RADIUS n'est pas disponible, le nom d'utilisateur et le mot de passe locaux sont vérifiés.

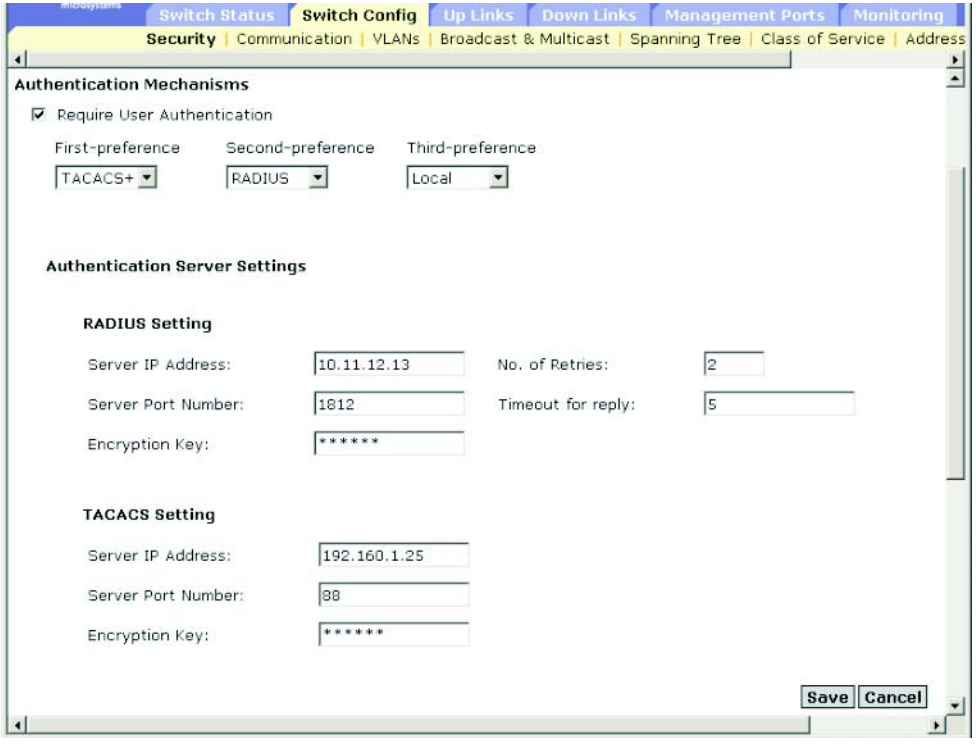
Attributs des commandes

- **Mécanismes d'authentification**
  - **Require User Authentication** : Indique si une authentification est requise.
  - **Preference** : Le commutateur tente d'authentifier l'utilisateur sur la base de la séquence spécifiée.

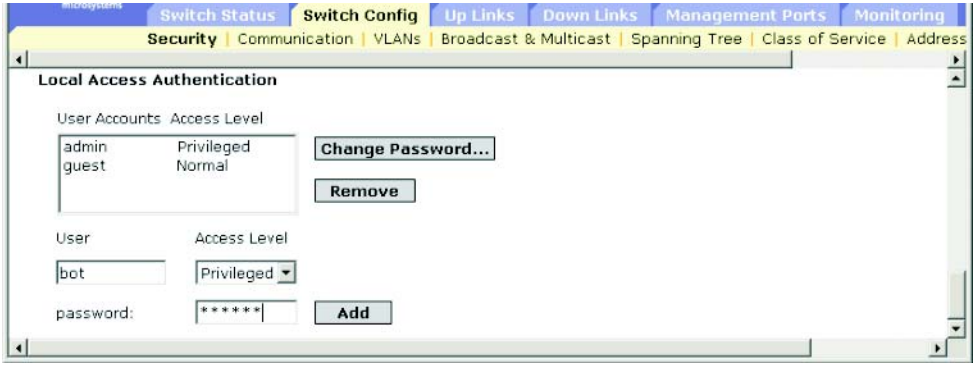
- **Paramètres du serveur d'authentification**
  - **Server IP Address** : Adresse du serveur d'authentification. (Par défaut : 10.1.0.1)
  - **Server Port Number :** Port réseau (UDP) du serveur d'authentification utilisé pour les messages d'authentification. (Plage : 1-65535 ; Par défaut : 1812)
  - **Encryption Key** : Clé de chiffrement utilisée pour authentifier les droits de connexion du client. Ne laissez pas d'espaces blancs dans la chaîne. (Longueur maximale : 20 caractères)
  - **No. of Retries*** : Nombre de tentatives effectuées par le commutateur pour authentifier les droits de connexion via le serveur d'authentification. (Plage : 1-30 ; Par défaut : 2)
  - **Timeout for reply*** : Nombre de secondes pendant lequel le commutateur attend une réponse avant de renvoyer une requête. (Plage : 1-65535 ; Par défaut : 5)
- **Authentification d'accès locale**
  - **User Account** : Nom de l'utilisateur. (Longueur maximale : 8 caractères ; nombre maximal d'utilisateurs : 5)
  - **Access Level** : Spécifie le niveau de l'utilisateur. (Options : Normal et Privileged.)
  - **Password** : Spécifie le mot de passe de l'utilisateur. (Longueur maximale : 8 caractères en texte simple, respectant la casse)

* Ne s'applique qu'à l'authentification par le biais du serveur RADIUS.

Web : Ouvrez Switch Config=>Security. Pour configurer des préférences d'authentification locales ou distantes, spécifiez la séquence d'authentification (à savoir une à trois méthodes), remplissez les paramètres des méthodes d'authentification spécifiés, et cliquez sur Save.



Pour configurer les paramètres d'authentification pour un accès local, entrez un nom d'utilisateur, un mot de passe et un niveau d'accès, puis cliquez sur Add.



ILC : Affectez un nom d'utilisateur et un niveau d'accès (à savoir 0 : Normal ; 15 : Privileged), puis spécifiez le mot de passe. Ensuite, configurez les paramètres requis pour l'authentification du client distant RADIUS et TACACS.

```
Console(config)#username bob access-level 15 4-26
Console(config)#username bob password smith
Console(config)#authentication login local tacacs radius 4-42
Console(config)#tacacs-server host 192.168.1.24 4-46
Console(config)#tacacs-server port 181 4-46
Console(config)#tacacs-server key green 4-47
Console(config)#radius-server host 192.168.1.25 4-43
Console(config)#radius-server port 181 4-43
Console(config)#radius-server key white 4-44
Console(config)#radius-server retransmit 5 4-44
Console(config)#radius-server timeout 10 4-45
Console(config)#
```

SNMP : Variables MIB équivalentes..

Nom de zone	Variable MIB	Accès	Plage de valeurs	Valeur par défaut
User Name	*Non défini*			
Password	*Non défini*			
Access Level	*Non défini*			
Authentication Sequence	*Non défini*			
RADIUS Server Address	sun... securityMgt.radiusMgt. radiusServerAddress	Lecture/ Ecriture	Adresse IP	10.11.12.13
RADIUS Server Port Number	sun... securityMgt.radiusMgt. radiusServerPortNumber	Lecture/ Ecriture	Nombre entier (1-65535)	1812
RADIUS Server Encryption Key	sun... securityMgt.radiusMgt. radiusServerKey	Lecture/ Ecriture (Indique toujours 0 en mode lecture)	Chaîne (Taille (0-20))	
RADIUS Server Retransmit	sun... securityMgt.radiusMgt. radiusServerRetransmit	Lecture/ Ecriture	Nombre entier (1-65535)	2
RADIUS Server Timeout	sun... securityMgt.radiusMgt. radiusServerTimeout	Lecture/ Ecriture	Nombre entier (1-65535) secondes	5

Nom de zone	Variable MIB	Accès	Plage de valeurs	Valeur par défaut
TACACS Server Address	sun... securityMgt.tacacsMgt. tacacsServerAddress	Lecture/ Ecriture	Adresse IP	
TACACS Server Port Number	sun... securityMgt.tacacsMgt. tacacsServerPortNumber	Lecture/ Ecriture	Nombre entier (1-65535)	
TACACS Server Encryption Key	sun... securityMgt.tacacsMgt. tacacsServerKey	Lecture/ Ecriture (Indique toujours 0 en mode lecture)	Chaîne (Taille (0-20))	

3.2.7 Configuration du protocole SNMP

Le protocole SNMP (Simple Network Management Protocol) est un protocole de communication conçu spécifiquement pour la gestion des périphériques et des autres éléments d'un réseau. Parmi les équipements généralement gérés par le biais du protocole SNMP, on trouve les commutateurs, les routeurs et les machines hôtes. Le protocole SNMP sert généralement à configurer ces périphériques pour un fonctionnement optimal dans un environnement de réseau ainsi qu'à les surveiller afin d'évaluer leurs performances ou de détecter des problèmes potentiels.

Le commutateur comprend un agent SNMP intégré qui surveille en permanence l'état de son matériel ainsi que le trafic passant par ces ports. Une station de gestion réseau peut accéder à ces informations à l'aide d'un logiciel tel que SunNet Manager. Les droits d'accès à l'agent intégré sont déterminés par des chaînes de communauté. Pour communiquer avec le commutateur, la station de gestion doit d'abord soumettre une chaîne de communauté valable à des fins d'authentification. Les options permettant de configurer les chaînes de communauté et les fonctions d'interruption associées sont décrites dans les sections suivantes.

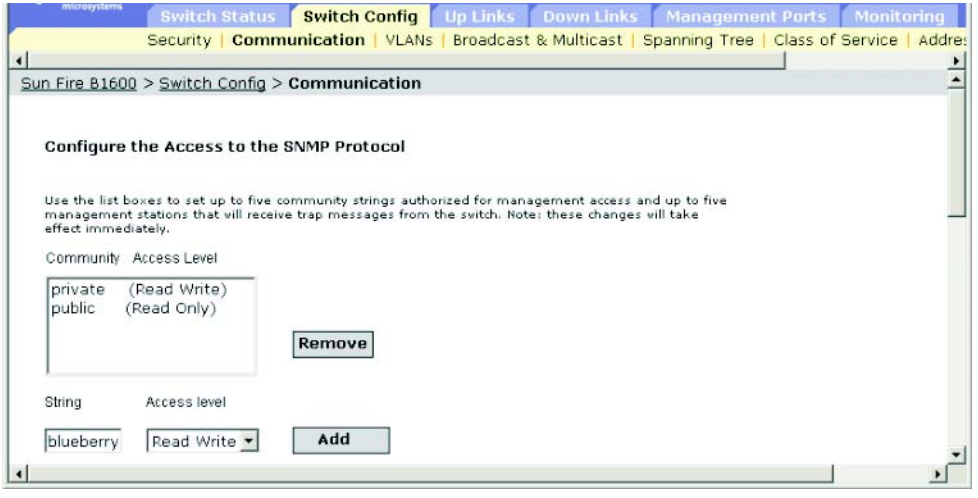
3.2.7.1 Configuration de l'accès au protocole SNMP

Vous pouvez configurer jusqu'à cinq chaînes de communauté autorisées pour l'accès à des fins de gestion. Pour des raisons de sécurité, nous vous conseillons de supprimer les chaînes par défaut.

Attributs des commandes

- **Community** : Une chaîne de communauté se comporte comme un mot de passe et autorise l'accès au protocole SNMP.
  Chaînes par défaut : « public » (accès en lecture seule), « private » (accès en lecture/écriture)
  - Plage : 1-32 caractères, respectant la casse
  - Valeurs par défaut : « public » (accès en lecture seule), « private » (accès en lecture/écriture)
- **Niveaux d'accès**
  - **Read Only** : Spécifie un accès en lecture seule. Les stations de gestion autorisées peuvent uniquement récupérer les objets MIB.
  - **Read/Write** : Spécifie un accès en lecture/écriture. Les stations de gestion autorisées peuvent récupérer et modifier les objets MIB.

Web : Ouvrez Switch Config=>Communication. Ajoutez les nouvelles chaînes de communauté requises, sélectionnez les droits d'accès depuis la liste déroulante Access Level (Niveaux d'accès), puis cliquez sur Add.



ILC : L'exemple suivant ajoute la chaîne « blueberry » avec un accès en lecture/écriture.

```
Console(config)#snmp-server community blueberry rw          4-48
Console(config)#
```

SNMP : Variables MIB équivalentes.

Il n'existe aucune variable MIB pour ces fonctions.

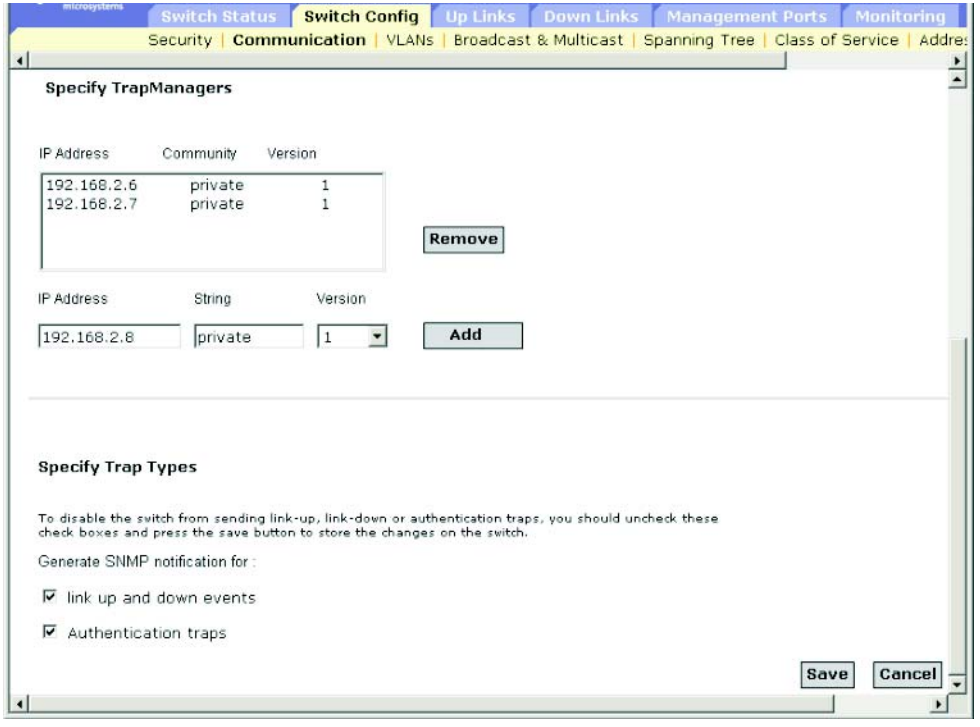
3.2.7.2 Spécification des gestionnaires d'interruptions et des types d'interruptions

Des interruptions indiquant les changements d'état sont émises par le commutateur à l'adresse des gestionnaires d'interruptions spécifiés. Vous devez spécifier des gestionnaires d'interruptions de telle sorte que les événements-clés soient notifiés par le commutateur à votre station de gestion (à l'aide de plates-formes de gestion réseau telles que SunNet Manager). Vous pouvez spécifier jusqu'à cinq stations de gestion destinées à recevoir des messages d'interruptions depuis le commutateur. Les interruptions prises en charge par ce commutateur sont reprises sous « Interruptions prises en charge » à la page A-3.

Attributs des commandes

- **IP Address** : Adresse Internet de l'hôte (destinataire cible).
  (Nbre max. d'adresses hôtes : 5 adresses IP de destination pour les interruptions)
- **Community :** Chaîne de communauté analogue à un mot de passe, envoyée avec l'opération de notification. Bien que vous puissiez configurer cette chaîne dans la table Trap Managers, nous vous recommandons de la définir également dans la table SNMP Protocol. (Longueur maximale : 32 caractères)
- **Version** : Indique si l'hôte utilise la version 1 ou 2c du protocole SNMP.
- **Génération de notification SNMP pour**
  - **Port link up and down events** : Emet un message d'interruption lorsqu'une liaison est établie ou interrompue au niveau du port.
  - **Authentication traps** : Emet un message d'interruption lorsqu'une chaîne de communauté non valable est soumise pendant le processus d'authentification d'accès au SNMP.

Web : Ouvrez Switch Setup=>Communications. Renseignez l'adresse IP et la chaîne de communauté pour chaque gestionnaire d'interruptions qui recevra ces messages, et cliquez sur Add. Marquez les événements de liaison ascendante et descendante du port ou la case à cocher Authentication traps si nécessaire, et cliquez sur Save.



ILC : Cet exemple ajoute un gestionnaire d'interruptions et active les interruptions de liaison ascendante/descendante et les interruptions d'authentification.

```
Console(config)#snmp-server host 10.1.0.19 private version 1 14-50
Console(config)#snmp-server enable traps link-up-down 4-51
Console(config)#snmp-server enable traps authentication
```

SNMP : Variables MIB équivalentes.

Nom de zone	Variable MIB	Accès	Plage de valeurs	Valeur par défaut
Trap Destination Address	sun... trapDestMgt. trapDestTable. trapDestEntry. trapDestAddress	Aucun accès	Adresse IP	
Trap Destination Community	sun... trapDestMgt. trapDestTable. trapDestEntry. trapDestCommunity	Lecture/ Création	Chaîne (Taille (0-127))	
Trap Destination Version	sun... trapDestMgt. trapDestTable. trapDestEntry. trapDestStatus	Lecture/ Création	version 1 (1), version 2 (2),	
Trap Destination Status	sun... trapDestMgt. trapDestTable. trapDestEntry. trapDestStatus	Lecture/ Création	valid (1), invalid (2)	
Enable Link-up-down Traps	MIB-II. ifMIB.ifMIBObjects. ifXTable.ifXEntry. ifLinkUpDownTrapEnable	Lecture/ Ecriture	enabled (1), disabled (2)	enabled

3.3 Configuration des protocoles Global Network

Cette section décrit comment configurer les paramètres globaux du commutateur pour les LAN virtuels, les services multidestinataires, l'algorithme Spanning Tree, la gestion des données sur la base des exigences des classes de services spécifiques ainsi que la manière d'afficher la table d'adressage ou de définir des adresses statiques.

3.3.1 Configuration des réseaux locaux virtuels

Dans les réseaux conventionnels avec routeurs, le trafic de diffusion est divisé en domaines distincts. Les commutateurs ne prennent pas en charge les domaines de diffusion de manière inhérente. Cette particularité peut entraîner l'apparition d'orages de diffusion dans les grands réseaux gérant d'importants volumes de trafic, tels que IPX ou NetBeui. Grâce aux réseaux locaux virtuels (VLAN) conformes à la norme IEEE 802.1Q, vous pouvez organiser vos groupes de noeuds réseau en domaines de diffusion distincts, confinant ainsi le trafic de diffusion au groupe d'origine. Vous obtenez ainsi un environnement réseau plus sûr et plus transparent.

Un VLAN conforme à la norme IEEE 802.1Q constitue un groupe de ports qui peuvent se situer partout sur le réseau, mais communiquent comme s'ils appartenaient au même segment physique.

Les VLAN contribuent à simplifier la gestion du réseau en vous permettant de déplacer des périphériques vers un nouveau VLAN sans devoir modifier les connexions physiques. Vous pouvez aisément organiser les VLAN pour que ceux-ci reflètent des groupes de services (tels que le Marketing ou la R&D), des groupes d'utilisations (par exemple, le courrier électronique) ou des groupes multidestinataires (utilisés pour des applications multimédia telles que les vidéoconférences).

Les VLAN accroissent l'efficacité du réseau en réduisant le trafic de diffusion et en vous permettant d'apporter des modifications au réseau sans devoir mettre à jour les adresses ou sous-réseaux IP. Les VLAN assurent un haut degré de sécurité réseau de manière inhérente, étant donné que le trafic doit traverser une liaison de couche 3 configurée avant d'atteindre un autre VLAN.

Ce commutateur prend en charge les fonctions VLAN suivantes :

- jusqu'à 255 VLAN basés sur la norme IEEE 802.1Q ;
- un apprentissage des VLAN distribué sur plusieurs commutateurs utilisant les méthodes de marquage explicite ou implicite ainsi que le protocole GVRP ;
- le chevauchement des ports, permettant à un port de participer à plusieurs VLAN ;
- la possibilité, pour les stations terminales, d'appartenir à plusieurs VLAN ;
- la transmission du trafic entre des périphériques prenant ou non les VLAN en charge ;
- le marquage des priorités.

Affectation de ports à des réseaux locaux virtuels

Avant d'activer des réseaux locaux virtuels pour le commutateur, vous devez affecter chaque port au(x) groupe(s) de VLAN auquel il participera. Par défaut, tous les ports sont affectés au VLAN 1 en tant que ports non marqués. Ajoutez un port en tant que port marqué si vous souhaitez gérer le trafic pour un ou plusieurs VLAN et si l'un des périphériques réseau intermédiaires ou l'hôte situé à l'autre extrémité de la connexion prend en charge les VLAN. Ensuite, affectez les ports des autres périphériques réseau reconnaissant les VLAN et situés sur le chemin emprunté par le trafic destiné au(x) même(s) VLAN. Cette affectation peut être manuelle ou dynamique (dans ce cas, vous utilisez le protocole GVRP). Toutefois, si vous souhaitez qu'un port de ce commutateur participe à un ou plusieurs VLAN, mais que les VLAN ne sont pris en charge ni par les périphériques réseau intermédiaires ni par l'hôte situé à l'autre extrémité de la connexion, ajoutez ce port au VLAN sous la forme d'un port non marqué.

Remarque - La transmission de trames portant une marque VLAN ne requiert pas que les périphériques d'interconnexion réseau prennent les VLAN en charge. Par contre, elles ne peuvent pas être utilisées pour les hôtes terminaux ne reconnaissant pas le marquage VLAN.

VLAN Classification : Lorsque le commutateur reçoit une trame, il la classifie de l'une des deux manières suivantes. Si la trame n'est pas marquée, le commutateur l'affecte à un VLAN associé (sur la base du PVID du port de réception). Dans le cas contraire, le commutateur utilise l'identificateur du VLAN marqué pour identifier le domaine de diffusion du port de la trame.

Port Overlapping : Le chevauchement des ports peut servir à permettre l'accès aux ressources réseau partagées par les différents groupes de VLAN, tels que les serveurs de fichiers ou les imprimantes. Remarquez que si vous mettez en oeuvre des VLAN qui ne se chevauchent pas, mais doivent néanmoins communiquer, vous pouvez les connecter à l'aide d'un commutateur ou d'un routeur de couche 3.

Port-based VLANs : Les VLAN basés sur le port (ou statiques) sont associés manuellement à des ports spécifiques. La décision de transmission du commutateur se fonde sur l'adresse MAC de destination ainsi que sur le port associé. C'est pourquoi, pour pouvoir prendre de bonnes décisions en matière de transmission et d'inondation, le commutateur doit apprendre la relation entre l'adresse MAC et le port associé - et donc avec le VLAN - au moment de l'exécution. Toutefois, lorsque le GVRP est activé, ce processus peut être entièrement automatisé.

Automatic VLAN Registration : Le protocole GVRP (GARP VLAN Registration Protocol) définit un système par le biais duquel le commutateur peut automatiquement apprendre quels VLAN doivent être associés à chaque station terminale. Si une station terminale (ou son adaptateur réseau) prend en charge le protocole VLAN IEEE 802.1Q, elle peut être configurée de manière à diffuser un message à votre réseau indiquant les groupes de VLAN qu'elle souhaite joindre. Lorsque ce commutateur reçoit ces messages, il place automatiquement le port de

réception dans les VLAN spécifiés, puis transmet les messages à tous les autres ports. Lorsque le message arrive à un autre commutateur prenant en charge le protocole GVRP, celui-ci agit de la même manière. Les exigences des VLAN sont ainsi propagées dans tout le réseau. Ceci permet de configurer automatiquement les périphériques compatibles GVRP pour les groupes de VLAN basés uniquement sur les requêtes de la station terminale.

Pour mettre le GVRP en oeuvre dans un réseau, commencez par ajouter les périphériques hôtes aux VLAN requis (à l'aide du système d'exploitation ou d'un autre logiciel d'application), de telle sorte que ces derniers puissent être propagés dans le réseau. Pour les commutateurs marginaux attachés directement à ces hôtes et les commutateurs principaux du réseau, activez le GVRP sur les liaisons entre ces périphériques. (Reportez-vous à la section « Configuration du comportement des VLAN pour les interfaces » à la page 3-93). Vous devez également déterminer des « frontières » dans le réseau à des fins de sécurité et désactiver le GVRP sur les ports des stations terminales où vous devez éviter la propagation des publicités ou interdire aux ports de contacter les VLAN à accès restreint.

Remarque - Si vous disposez de périphériques hôtes ne prenant pas le GVRP en charge, vous devez configurer des VLAN statiques pour les ports du commutateur connectés à ceux-ci (tel que décrit dans « Ajout de membres statiques aux réseaux locaux virtuels » à la page 3-42). Mais vous devez avoir la possibilité d'activer le GVRP sur ces commutateurs de périphérie, de même que sur les commutateurs principaux du réseau.

Transmission de trames marquées/non marquées

Si vous souhaitez créer un petit réseau local virtuel basé sur les ports pour les périphériques attachés directement à un seul commutateur, vous devez affecter les ports au même VLAN non marqué. Toutefois, pour participer à un groupe de VLAN couvrant plusieurs commutateurs, vous devez créer un VLAN pour ce groupe et activer le marquage sur tous les ports.

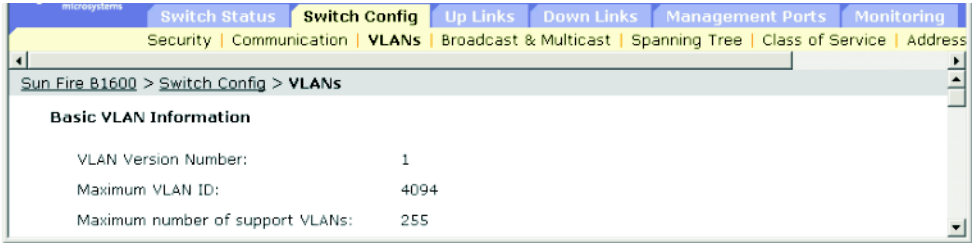
Les ports peuvent être affectés à plusieurs VLAN marqués ou non marqués. Chaque port du commutateur est donc à même de transmettre des trames marquées ou non marquées. Lorsque vous transmettez une trame depuis ce commutateur le long d'un chemin contenant des périphériques prenant les VLAN en charge, le commutateur doit inclure des marques VLAN. Si aucun des périphériques ne prend les VLAN en charge (y compris l'hôte de destination), le commutateur doit d'abord retirer toutes les marques VLAN avant de transmettre la trame. Lorsque le commutateur reçoit une trame marquée, il la transmet au(x) VLAN indiqué(s) par la marque. Toutefois, lorsque ce commutateur reçoit une trame non marquée d'un périphérique ne prenant pas les VLAN en charge, il doit d'abord décider de la destination de la trame, puis insérer une marque représentant le VID par défaut du port d'entrée.

3.3.1.1 Affichage d'informations de base sur les réseaux locaux virtuels

Attributs des commandes

- **VLAN Version Number** : Version du VLAN utilisée par ce commutateur telle que spécifiée dans la norme IEEE 802.1Q.
- **Maximum VLAN ID** : Identificateur maximal du VLAN reconnu par ce commutateur.
- **Maximum Number of Supported VLANs** : Nombre maximal de VLAN pouvant être configurés sur ce commutateur.

Web : Ouvrez Switch Config=>VLANs.



ILC : Entrez la commande suivante.

```
Console#show bridge-ext4-120
 Max support vlan numbers: 32
 Max support vlan ID: 4094
 Extended multicast filtering services: No
 Static entry individual port: Yes
 VLAN learning: IVL
 Configurable PVID tagging: Yes
 Local VLAN capable: Yes
 Traffic classes: Enabled
 Global GVRP status: Disabled
 GMRP: Disabled
Console#
```

SNMP : Variables MIB équivalentes.

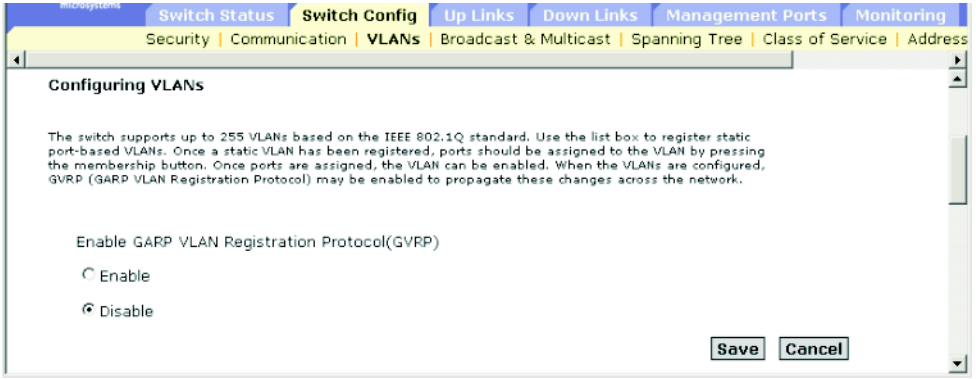
Nom de zone	Variable MIB	Accès	Plage de valeurs	Valeur par défaut
VLAN Version Number	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qBase. dot1qVlanVersion-Number	Lecture seule	version1 (1)	version1

Nom de zone	Variable MIB	Accès	Plage de valeurs	Valeur par défaut
Maximum VLAN ID	MIB-II. dot1dBridge. BridgeMIB. BridgeMIBObjects. dot1qBase. dot1qMaxVlanId	Lecture seule	Nombre entier	4094
Maximum Number of Supported VLANs	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qBase. dot1qMaxSupportedVlans	Lecture seule	Nombre entier	255
Device Capabilities	MIB-II. dot1dBridge. pBridgeMIB. pBridgeMIBObjects. dot1dExtBase. dot1dDeviceCapabilities	Lecture seule	Bit String – ExtendedFiltering dot1dServices (0), dot1dTrafficClasses (1), StaticEntry dot1dIndividualPort (2), dot1dIVLCapable (3), dot1dSVLCapable (4), dot1dHybridCapable (5), dot1dConfigurablePvid dot1dTagging (6), dot1dLocalVlanCapable (7)	2, 3, 6, 7
Traffic Classes Enabled	MIB-II. dot1dBridge. pBridgeMIB. pBridgeMIBObjects. dot1dExtBase. dot1dTrafficClasses-Enabled	Lecture/ Ecriture	true (1), false (2)	true
GMRP Status	MIB-II. dot1dBridge. pBridgeMIB. pBridgeMIBObjects. dot1dExtBase. dot1dGmrpStatus	Lecture/ Ecriture	enabled (1), disabled (2)	disabled
GVRP Status	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qBase. dot1qGvrpStatus	Lecture/ Ecriture	enabled (1), disabled (2)	disabled

3.3.1.2 Activation ou désactivation du GVRP (Global Setting)

Le protocole GVRP (GARP VLAN Registration Protocol) définit une méthode permettant aux commutateurs d'échanger des informations sur les VLAN afin d'enregistrer les membres des VLAN sur tous les ports du réseau. Les VLAN sont configurés de manière dynamique sur la base de messages communs émis par les périphériques hôtes et propagés sur le réseau. Le protocole GVRP doit être activé pour permettre un enregistrement automatique des VLAN et pour pendre en charge les VLAN allant au-delà du commutateur local.

Web : Ouvrez Switch Config=>VLANs. Activez ou désactivez le GVRP, puis cliquez sur Save.



ILC : Cet exemple active le GVRP pour le commutateur.

```
Console(config)#bridge-ext gvrp4-119
Console(config)#
```

SNMP : Variables MIB équivalentes.

Nom de zone	Variable MIB	Accès	Plage de valeurs	Valeur par défaut
GVRP Status	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qBase. dot1qGvrpStatus	Lecture/ Ecriture	enabled (1), disabled (2)	disabled

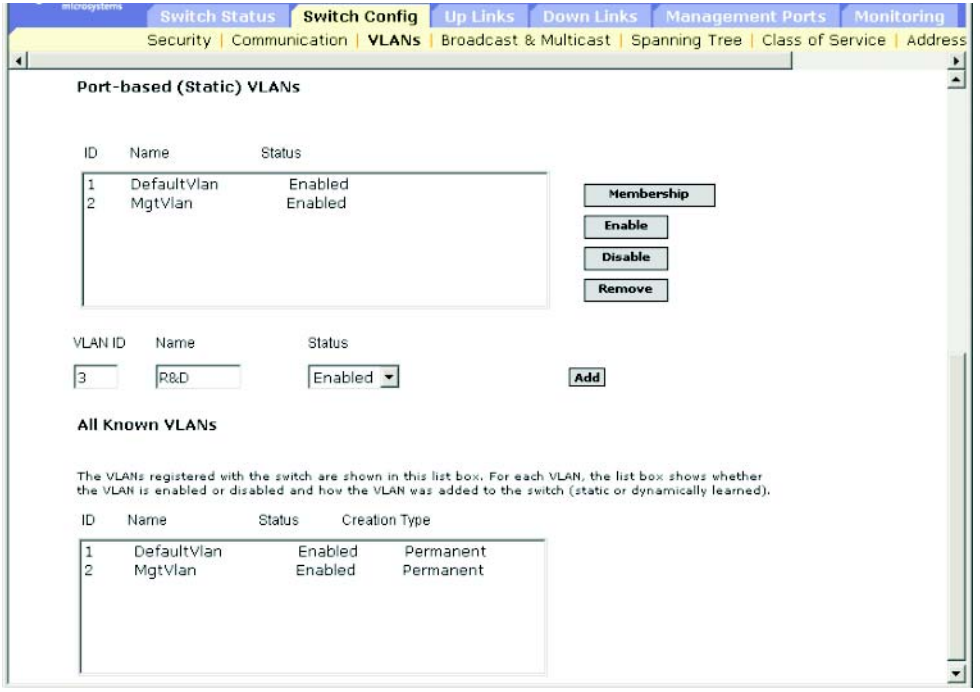
3.3.1.3 Configuration des réseaux locaux virtuels

Attributs des commandes

- **ID** : ID du VLAN configuré (1-4094).
- **Name** : Nom du VLAN (1 à 15 caractères).
- **Status** : Indique si ce VLAN est activé ou désactivé.
  - **Enable** (Active*) : VLAN actif.
  - **Disable** (Suspend*) : VLAN désactivé - en d'autres termes, il ne transmet pas de paquets.
- **Creation Type** : Montre comment ce VLAN a été ajouté au commutateur.
  - **Dynamic GVRP** (Dynamic*) : Apprentissage automatique via GVRP.
  - **Permanent** (Static*) : Ajouté en tant qu'entrée statique.
- **Ports / Channel groups*** : Affiche les membres de l'interface du VLAN.

* L'ILC affiche ces termes.

Web : Ouvrez Switch Config=>VLANs. Pour créer un nouveau VLAN, entrez son identificateur et son nom, configurez un état Enabled ou Disabled, puis cliquez sur Add. Pour modifier des VLAN existants, sélectionnez une ou plusieurs entrées, cliquez sur Enable, Disable ou Remove. Pour ajouter des interfaces à un VLAN, sélectionnez une entrée et cliquez sur Membership. (Voir « Ajout de membres statiques aux réseaux locaux virtuels » à la page 3-42.)



ILC : L'exemple suivant crée un nouveau VLAN et affiche toutes les informations sur le VLAN.

```
Console(config)#vlan database4-106
Console(config-vlan)#vlan 3 name R&D media ethernet state active4-106
Console(config-vlan)#
Console#show vlan4-114
VLAN Type    Name             Status    Ports/Channel groups
---- ------- ---------------- --------- ---------------------------------------
   1  Static      DefaultVlan    Active    SNP0    SNP1    SNP2    SNP3    SNP4
                                           SNP5    SNP6    SNP7    SNP8    SNP9
                                          SNP10   SNP11   SNP12   SNP13   SNP14
                                          SNP15   NETP0   NETP1   NETP2   NETP3
                                          NETP4   NETP5   NETP6   NETP7
   2  Static          MgtVlan    Active  NETMGT
   3  Static              R&D    Active
Console#
```

SNMP : Variables MIB équivalentes.

Nom de zone	Variable MIB	Accès	Plage de valeurs	Valeur par défaut
VLAN ID	MIB-II.dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanCurrentTable. dot1qVlanCurrentEntry. dot1qVlanIndex	Aucun accès	Nombre entier	1
VLAN Name	MIB-II.dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanStaticTable. dot1qVlanStaticEntry. dot1qVlanStaticName	Lecture/ Création	Chaîne d'octets (Taille (0-32))	
VLAN Status	MIB-II.dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanStaticTable. dot1qVlanStaticEntry. dot1qVlanStatic. RowStatus	Lecture/ Création	enable(1), disable(2)	
VLAN Type	MIB-II.dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanCurrentTable. dot1qVlanCurrentEntry. dot1qVlanStatus	Lecture seule	other(1), permanent(2), dynamicGvrp(3)	

Nom de zone	Variable MIB	Accès	Plage de valeurs	Valeur par défaut
VLAN Ports	MIB-II.dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanCurrentTable. dot1qVlanCurrentEntry. dot1qVlanCurrent-EgressPorts	Lecture seule	Chaîne d'octets (Liste des ports)	

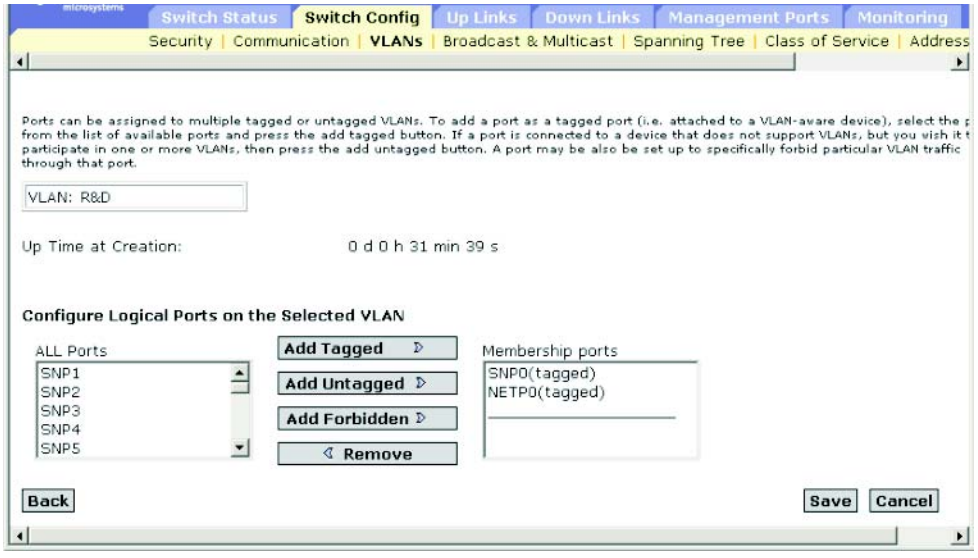
3.3.1.4 Ajout de membres statiques aux réseaux locaux virtuels

Attributs des commandes

- **Name** : Nom du VLAN.
- **Up Time at Creation** : Heure de création de ce VLAN.
- **Status*** : Méthode d'ajout de ce VLAN au commutateur.
  - **Dynamic** : Apprentissage automatique via GVRP.
  - **Static** : Ajout en tant qu'entrée statique.
- **All Ports** : ID des ports ou des groupes.
- **Membership Ports** : Interfaces ajoutées au VLAN sélectionné sous une forme marquée ou non, ou ne pouvant être ajoutées automatiquement via le GVRP.
- **Membership Type** : Spécifiez l'appartenance au VLAN en sélectionnant l'interface requise, puis cliquez sur le bouton Add approprié :
  - **Add Tagged** : L'interface est membre du VLAN. Tous les paquets transmis par le port sur ce VLAN sont marqués. En d'autres termes, ils sont porteurs d'une marque et contiennent donc des informations sur le VLAN ou la CdS.
  - **Add Untagged** : L'interface est membre du VLAN. Aucun paquet transmis par le port sur ce VLAN n'est marqué. En d'autres termes, ils ne sont pas porteurs de marque et ne contiennent donc pas d'informations sur le VLAN ou la CdS.
  - **Add Forbidden** : Il est interdit à l'interface d'adhérer au VLAN automatiquement via le GVRP. Reportez-vous à « Enregistrement automatique du VLAN » à la page 4-35.
  - **Remove** : Supprime l'interface sélectionnée de ce VLAN.

* ILC uniquement.

Web : Ouvrez Switch Config=>VLANs. Sélectionnez un VLAN dans la liste statique, puis cliquez sur Membership. Sur la page Port membership, sélectionnez une interface dans la liste All Ports (à savoir port ou groupe), et cliquez sur Add Tagged, Add Untagged ou Add Forbidden (c'est-à-dire empêcher que cette interface soit ajoutée par le biais du GVRP). Pour supprimer une interface, sélectionnez une entrée dans la liste Membership Ports, puis cliquez sur Remove.



ILC : Cet exemple ajoute plusieurs interfaces, puis affiche les membres du VLAN.

```
Console(config)#interface ethernet NETP14-74
Console(config-if)#switchport allowed vlan add 3 tagged4-112
Console(config-if)#exit
Console(config)#interface ethernet NETP2
Console(config-if)#switchport allowed vlan add 3 untagged
Console(config-if)#exit
Console(config)#interface ethernet SNP13
Console(config-if)#switchport forbidden vlan add 3
Console(config-if)#end
Console#show vlan id 3
VLAN Type    Name             Status    Ports/Channel groups
---- ------- ---------------- --------- -------------------------
   3  Static              R&D    Active   NETP1   NETP2
Console#
```

SNMP : Variables MIB équivalentes.

Nom de zone	Variable MIB	Accès	Plage de valeurs	Valeur par défaut
VLAN ID	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanStaticTable. dot1qVlanStaticEntry. dot1qVlanIndex	Index	Ligne	
VLAN Name	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanStaticTable. dot1qVlanStaticEntry. dot1qVlanStaticName	Lecture/ Création	Chaîne d'octets (Taille (0-32))-	
Up Time at Creation	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanCurrentTable. dot1qVlanCurrentEntry. dot1qVlanCreationTime	Lecture seule	Temps (en centisecondes)	
VLAN Status	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanCurrentTable. dot1qVlanCurrentEntry. dot1qVlanStatus	Lecture seule	other(1), permanent(2), dynamicGvrp(3)	
Tagged Ports, Untagged Ports (Allowed VLAN)	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanTable. dot1qVlanEntry. dot1qVlanStatic- UntaggedPorts	Lecture/ Création	Chaîne d'octets (Liste des ports)	

Nom de zone	Variable MIB	Accès	Plage de valeurs	Valeur par défaut
VLAN Forbidden Ports	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qPortVlanTable. dot1qPortVlanEntry. dot1qVlanForbidden-EgressPorts	Lecture/ Création	Chaîne d'octets (Liste des ports)	
Port Trunk Index (Channel Groups)	sun... portMgt. portTable portEntry. portTrunkIndex	Lecture seule	Nombre entier	
VLAN Static Row Status	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanStaticTable. dot1qVlanStaticEntry. dot1qVlanStatic-RowStatus	Lecture/ Création	enable(1), disable(2)	

3.3.2 Configuration multidestinataire

La configuration multidestinataire permet de prendre en charge des applications en temps réel telles que les vidéoconférences ou l'audio en flux continu. Un serveur multidestinataire ne doit pas établir de connexion distincte avec chaque client. Il lui suffit de diffuser ses services sur le réseau, et tous les hôtes désireux de recevoir ces services s'enregistrent auprès de leur commutateur/routeur multidestinataire local. Bien que cette approche réduise la surcharge du réseau induite par un serveur multidestinataire, le trafic diffusé doit être élagué avec prudence à chaque commutateur/routeur multidestinataire par lequel il passe afin de vérifier que le trafic n'est transmis qu'aux hôtes abonnés à ce service.

Le commutateur utilise le protocole IGMP (Internet Group Management Protocol) pour rechercher tout hôte attaché souhaitant recevoir un service multidestinataire spécifique. Il identifie les ports contenant des hôtes demandant à recevoir le service et n'envoie des données qu'à ces ports. Ensuite, il propage la requête de service à tout commutateur/routeur multidestinataire avoisinant afin de s'assurer qu'il continuera à recevoir le service multidestinataire. Cette procédure s'appelle le filtrage multidestinataire.

L'objectif du filtrage multidestinataire consiste à optimiser les performances d'un réseau commuté, de telle sorte que les paquets multidestinataires ne soient transmis qu'aux ports contenant des hôtes de groupes multidestinataires ou des routeurs/commutateurs multidestinataires, au lieu de transmettre le trafic à tous les ports du sous-réseau (VLAN).

3.3.2.1 Configuration des paramètres IGMP Snooping

Vous pouvez configurer le commutateur afin que celui-ci transmette le trafic multidestinataire intelligemment. Sur la base de la requête IGMP et des messages de notification, le commutateur ne transmet le trafic qu'aux ports demandant le trafic multidestinataire. Ce paramétrage empêche que le commutateur ne diffuse le trafic à tous les ports, risquant ainsi d'amoindrir les performances du réseau.

Utilisation de la commande

- **IGMP Snooping** : Ce commutateur peut surveiller passivement les paquets IGMP Query et Report transférés entre les routeurs/commutateurs multidestinataires IP et les groupes d'hôtes multidestinataires IP pour identifier les membres du groupe multidestinataire IP. Il contrôle simplement les paquets IGMP transitant par lui, prélève les informations sur l'enregistrement des groupes et configure les filtres multidestinataires en conséquence.
- **IGMP Querier** : Un routeur, ou commutateur multidestinataire, peut périodiquement demander à ses hôtes s'ils souhaitent recevoir le trafic multidestinataire. Si le réseau local comporte plus d'un routeur/commutateur se chargeant du trafic multidestinataire IP, l'un de ceux-ci est défini comme « requêteur » et se charge de lancer des requêtes au LAN pour connaître les membres du groupe. Ensuite, il propage la requête de service à tout commutateur/routeur multidestinataire en amont afin de s'assurer qu'il continuera à recevoir le service multidestinataire.

Remarque - Les routeurs multidestinataires utilisent ces informations ainsi qu'un protocole de routage multidestinataire tel que DVMRP pour prendre en charge le trafic multidestinataire sur Internet.

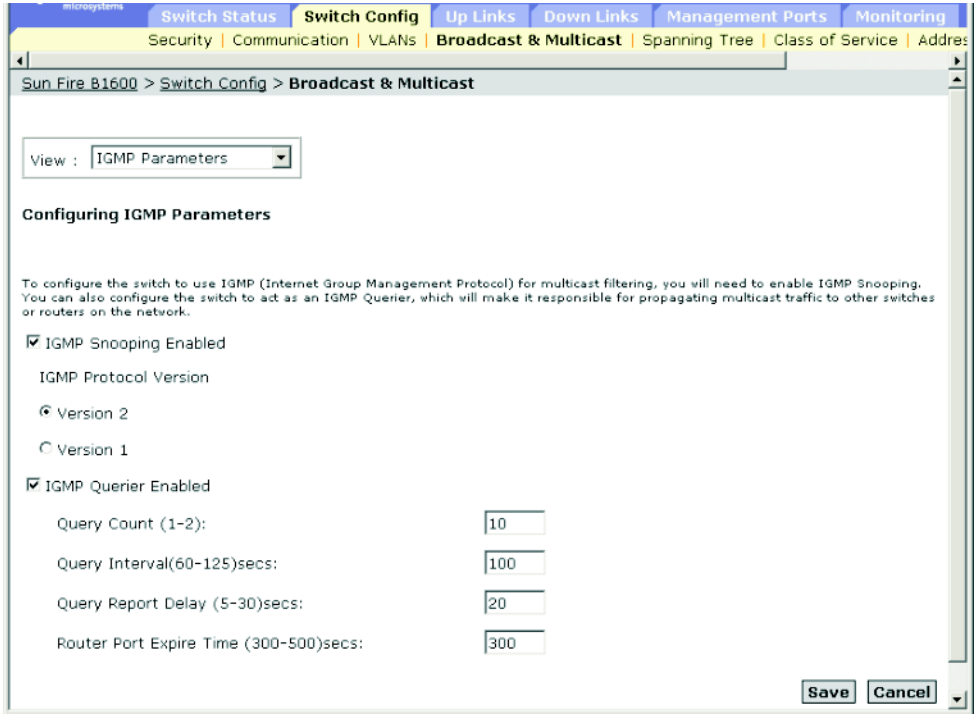
Attributs des commandes

- **IGMP Snooping** : Lorsque cette option est activée, le commutateur surveille le trafic réseau afin de déterminer quels hôtes souhaitent recevoir le trafic multidestinataire. (Par défaut : désactivé)
- **IGMP Protocol Version** : Définit la version du protocole afin de s'assurer de sa compatibilité avec les autres périphériques du réseau. (Par défaut : 2, Plage : 1-2)
- **IGMP Querier** : Lorsque cette fonction est activée, le commutateur peut servir de requêteur. En d'autres termes, il se charge de demander aux hôtes s'ils souhaitent recevoir le trafic multidestinataire. (Par défaut : désactivé)

- **Query Count** : Définit le nombre maximum de requêtes émises sans réponse avant que le requêteur exclue un client du groupe multidestinataire. (Par défaut : 2, Plage : 2-10)
- **Query Interval** : Définit la fréquence à laquelle le commutateur envoie des messages de requête d'hôte IGMP. (Par défaut : 125 secondes, Plage : 60-125)
- **Query Report Delay** : Définit le délai entre la réception d'un rapport IGMP pour une adresse IP multidestinataire sur un port et le moment où le commutateur envoie une requête IGMP depuis ce port et supprime l'entrée de sa liste. (Par défaut : 10 secondes, Plage : 5-25)
- **Router Port Expire Time** : Délai pendant lequel le commutateur attend après l'arrêt de l'envoi de requêtes par un requêteur avant de déterminer que l'interface (qui recevait les paquets de requêtes) n'est plus connectée à un requêteur. (Par défaut : 300 secondes, Plage : 300-500)

Remarque - Tous les systèmes du sous-réseau doivent prendre en charge la même version. Certains attributs ne sont activés que pour IGMPv2, y compris IGMP Report Delay et Router Port Expire Time.

Web : Cliquez sur Switch Config=>Broadcast & Multicast=>IGMP Parameters. Modifiez les paramètres IGMP requis, puis cliquez sur Save.



ILC : Cet exemple modifie les paramètres pour le filtrage multidestinataire, puis affiche l'état courant.

```
Console(config)#ip igmp snooping4-122
Console(config)#ip igmp snooping querier                          4-125
Console(config)#ip igmp snooping query-count 104-126
Console(config)#ip igmp snooping query-interval 1004-127
Console(config)#ip igmp snooping query-max-response-time 204-128
Console(config)#ip igmp router-port-expire-time 300               4-129
Console(config)#ip igmp snooping version 2                        4-123
Console(config)#exit
Console#show ip igmp snooping                                     4-124
 Igmp Snooping Configuration
 ---------------------------------------------
 Service status          : Enabled
 Querier status          : Enabled
 Query count             : 10
 Query interval          : 100 sec
 Query max response time : 20 sec
 Query time-out          : 300 sec
 IGMP snooping version   : Version 2
Console#
```

SNMP : Variables MIB équivalentes.

Nom de zone	Variable MIB	Accès	Plage de valeurs	Valeur par défaut
Snooping Status	sun... igmpSnoopMgt. igmpSnoopStatus	Lecture/ Ecriture	enabled (1), disabled (2)	enabled
Snooping Querier	sun... igmpSnoopMgt. igmpSnoopQuerier	Lecture/ Ecriture	enabled (1), disabled (2)	enabled
Snooping Query Count	sun... igmpSnoopMgt. igmpSnoopQueryCount	Lecture/ Ecriture	Nombre entier (2-10)	2
Snooping Query Interval	sun... igmpSnoopMgt. igmpSnoop-QueryInterval	Lecture/ Ecriture	Nombre entier (60-125) secondes	125
Snooping Query Max Response Time	sun... igmpSnoopMgt. igmpSnoopQuery-MaxResponseTime	Lecture/ Ecriture	Nombre entier (5-25) secondes	10

Nom de zone	Variable MIB	Accès	Plage de valeurs	Valeur par défaut
Snooping Router Port Expire Time	sun... igmpSnoopMgt. igmpSnoopRouterPort-ExpireTime	Lecture/ Ecriture	Nombre entier (300-500) secondes	300
Snooping Version	sun... igmpSnoopMgt. igmpSnoopVersion	Lecture/ Ecriture	Nombre entier (1-2)	2

3.3.2.2 Spécification des interfaces attachées à un routeur multidestinataire

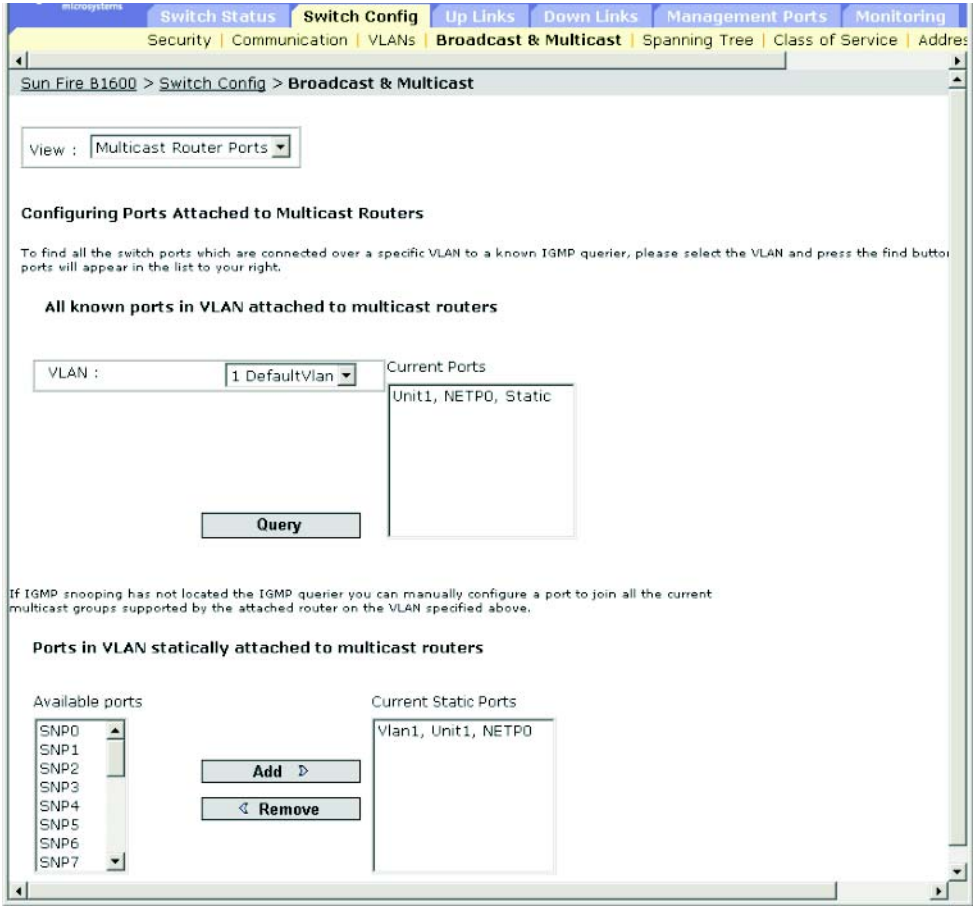
Les routeurs multidestinataires utilisent les informations obtenues par IGMP Query, ainsi qu'un protocole de routage multidestinataire tel que DVMRP, pour prendre en charge le trafic multidestinataire sur Internet. Ces routeurs peuvent être détectés de manière dynamique par le commutateur ou affectés de manière statique à une interface du réseau.

Selon vos connexions réseau, la surveillance IGMP peut ne pas toujours être en mesure de localiser le requêteur IGMP. C'est la raison pour laquelle, si le requêteur IGMP est un routeur/commutateur multidestinataire connu et connecté à une interface (port ou groupe du commutateur) par le biais du réseau, vous pouvez configurer manuellement l'interface (et un VLAN spécifié) pour qu'elle adhère à tous les groupes multidestinataires courants pris en charge par le routeur. Cette opération garantit que le trafic multidestinataire est transmis à toutes les interfaces appropriées du réseau.

Attribut de commande

- Tous les ports connus du VLAN attachés à des routeurs multidestinataires **:**
  - **VLAN** : Sélectionne un VLAN sur ce commutateur. (La liste déroulante contient l'identificateur du VLAN et son nom).
  - **Interface** : Affiche les interfaces attachées à un routeur multidestinataire, et la nature de l'affectation (statique (Static) ou dynamique (IGMP)).
- Ports du VLAN attachés à des routeurs multidestinataires de manière statique **:**
  - **Available Ports** : Affiche les interfaces qui n'ont pas été affectées au VLAN sélectionné en tant que port de routage.
  - **Current Static Ports** : Affiche les interfaces déjà affectées au VLAN sélectionné comme port du routage multidestinataire.

Web : Cliquez sur Switch Config=>Broadcast & Multicast=>Multicast Router Ports. Sélectionnez un VLAN, puis cliquez sur Query pour afficher toutes les interfaces du VLAN attachées à des routeurs multidestinataires ou utilisez les boutons Add/Remove pour attacher statiquement une interface à un routeur multidestinataire.



ILC : Cet exemple configure le port NETP0 comme port de routage multidestinataire sur le VLAN 1.

```
Console(config)#ip igmp snooping vlan 1 mrouter ethernet NETP0   4-130
Console(config)#exit
Console#show ip igmp snooping mrouter vlan 1                     4-131
 VLAN M'cast Router Port Type
 ---- ----------------- -------
    1              NETP0 Static
```

SNMP : Variables MIB équivalentes.

Nom de zone	Variable MIB	Accès	Plage de valeurs
Snooping Multicast Router Current VLAN	sun... igmpSnoopMgt. igmpSnoopRouterCurrentTable. igmpSnoopRouterCurrentEntry. dot1qVlanIndex	Index	Nombre entier
VLAN Name	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanStaticTable. dot1qVlanStaticEntry. dot1qVlanStaticName	Lecture/ Création	Chaîne d'octets (Taille (0-32))-
Snooping Multicast Router Current Ports	sun... igmpSnoopMgt. igmpSnoopRouterCurrentTable. igmpSnoopRouterCurrentEntry. igmpSnoopRouterCurrentPorts	Lecture seule	Chaîne d'octets (Port List)
Snooping Multicast Router Static Vlan Index	sun... igmpSnoopMgt. igmpSnoopRouterStaticTable. igmpSnoopRouterStaticEntry. dot1qVlanIndex	Index	Nombre entier
Snooping Multicast Router Static Ports	sun... igmpSnoopMgt. igmpSnoopRouterStaticTable. igmpSnoopRouterStaticEntry. igmpSnoopRouterStaticPorts	Lecture/ Création	Chaîne d'octets (Port List)
Snooping Multicast Router Static Status	sun... igmpSnoopMgt. igmpSnoopRouterStaticTable. igmpSnoopRouterStaticEntry. igmpSnoopRouterStaticStatus	Lecture/ Création	valid (1), invalid(2)

3.3.2.3 Configuration de services multidestinataires

Le filtrage multidestinataire peut être configuré de manière dynamique à l'aide des messages IGMP Snooping et IGMP Query, comme décrit dans « Configuration des paramètres IGMP Snooping » à la page 3-46. Pour certaines applications requérant un contrôle plus strict, il est possible que vous deviez affecter manuellement un service multidestinataire à une interface spécifique. Commencez par ajouter tous les ports attachés aux hôtes participants à un LAN virtuel commun, puis affectez un service multidestinataire à ce groupe de VLAN.

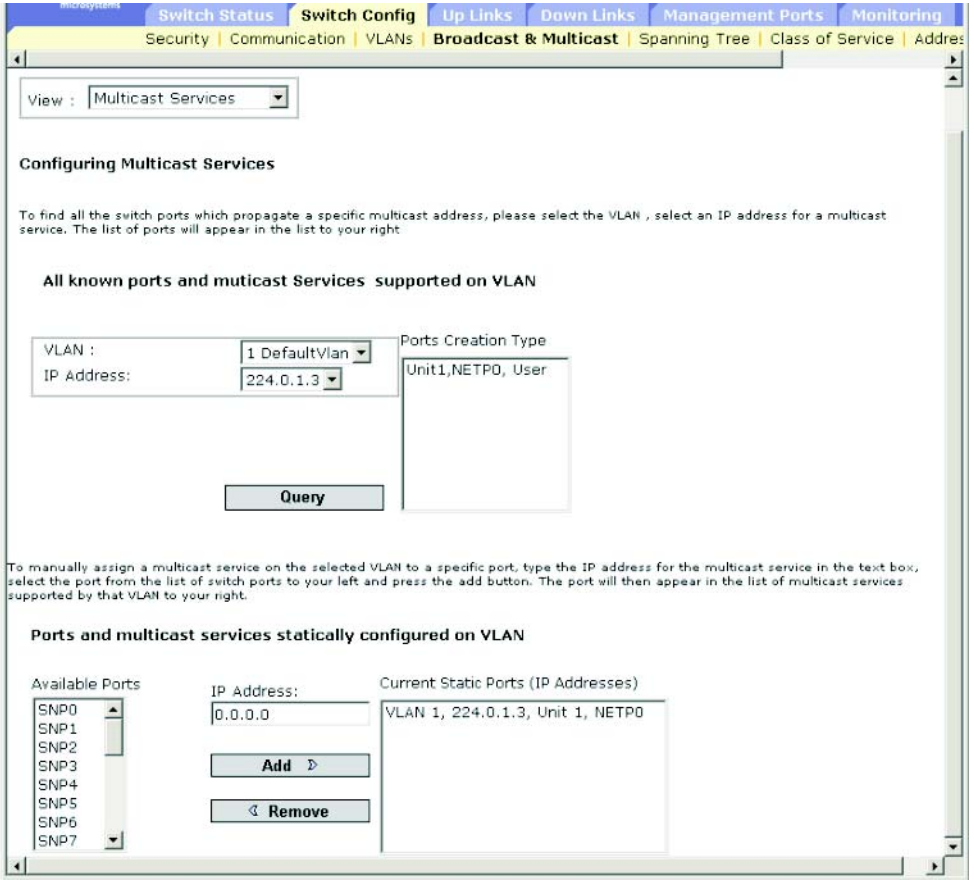
Utilisation de la commande

- Les adresses multidestinataires statiques ne deviennent jamais obsolètes.
- Lorsqu'une adresse multidestinataire est statistiquement affectée à une interface d'un VLAN spécifique, le trafic correspondant ne peut être transmis qu'aux ports de ce VLAN.

Attribut de commande

- Tous les ports connus et services multidestinataires pris en charge sur le VLAN :
  - **VLAN** : Sélectionne un VLAN sur ce commutateur.
    (La liste déroulante contient l'identificateur du VLAN et son nom).
  - **IP Address** : Adresse IP d'un service multidestinataire spécifique.
  - **Interface** : Affiche les interfaces attachées à un routeur multidestinataire, et la nature de l'affectation (statique (User) ou dynamique (IGMP)).
- Ports et services multidestinataires configurés de manière statique sur le VLAN :
  - **IP Address :** Adresse IP d'un service multidestinataire spécifique.
  - **Available Ports** : Affiche les interfaces qui n'ont pas été affectées au VLAN sélectionné pour prendre en charge un service multidestinataire spécifique.
  - **Current Static Ports (IP Addresses)** : Affiche les interfaces qui ont déjà été affectées au VLAN sélectionné pour propager un service multidestinataire spécifique. Affiche également l'adresse IP affectée à cette interface.

Web : Cliquez sur Switch Config=>Broadcast & Multicast=>Multicast Support. Pour afficher les interfaces du commutateur qui propagent un service multidestinataire spécifique, sélectionnez un identificateur de VLAN et l'adresse IP pour un service multidestinataire dans les listes déroulantes, puis cliquez sur Query. Pour affecter manuellement un service multidestinataire à une interface spécifique, sélectionnez un VLAN dans la liste déroulante, entrez l'adresse IP du service multidestinataire dans la zone de texte, puis cliquez sur Add.



Remarque - Si vous recevez un message d'erreur vous indiquant que les données saisies ne sont pas valables, vérifiez chacune des adresses IP.

ILC : Cet exemple affecte une adresse multidestinataire au port NETP0, puis affiche tous les services multidestinataires connus pris en charge sur le VLAN 1.

```
Console(config)#ip igmp snooping vlan 1 static 224.0.0.12 ethernet NETP0 4-123
Console(config)#exit
Console#show mac-address-table multicast vlan 1                          4-125
 VLAN M'cast IP addr. Member ports Type
 ---- --------------- ------------ -------
    1      224.0.0.12        NETP1    IGMP
    1       224.1.2.3        NETP0    USER
Console#
```

SNMP : Variables MIB équivalentes.

Nom de zone	Variable MIB	Accès	Plage de valeurs
Snooping Multicast Router Static Vlan Index	sun... igmpSnoopMgt. igmpSnoopMulticastStaticTable. igmpSnoopMulticastStaticEntry. dot1qVlanIndex	Index	Nombre entier
Snooping Multicast Static IP Address	sun... igmpSnoopMgt. igmpSnoopMulticastStaticTable. igmpSnoopMulticastStaticEntry. igmpSnoopMulticastStaticIPAddress	Index	Adresse IP
Snooping Multicast Static Port List	sun... igmpSnoopMgt. igmpSnoopMulticastStaticTable. igmpSnoopMulticastStaticEntry. igmpSnoopMulticastStaticPorts	Lecture/ Création	Chaîne d'octets (Liste des ports)
Snooping Multicast Router Static Status	sun... igmpSnoopMgt. igmpSnoopRouterStaticTable. igmpSnoopRouterStaticEntry. igmpSnoopRouterStaticStatus	Lecture/ Création	valid (1), invalid(2)

3.3.3 Contrôle des orages de diffusion (Global Setting)

Des orages de diffusion peuvent survenir lorsqu'un périphérique de votre réseau fonctionne mal, ou si des programmes d'application ne sont pas bien conçus ou mal configurés. S'il y a trop de trafic de diffusion sur votre réseau, les performances de celui-ci peuvent être considérablement amoindries ou le système peut complètement se bloquer.

Vous pouvez protéger votre réseau de ce type de problèmes en définissant un seuil relatif au trafic de diffusion s'appliquant à chaque port, puis en activant le contrôle des orages de diffusion sur les ports requis.

Tous les paquets de diffusion dépassant le seuil spécifié sont abandonnés.

Utilisation de la commande

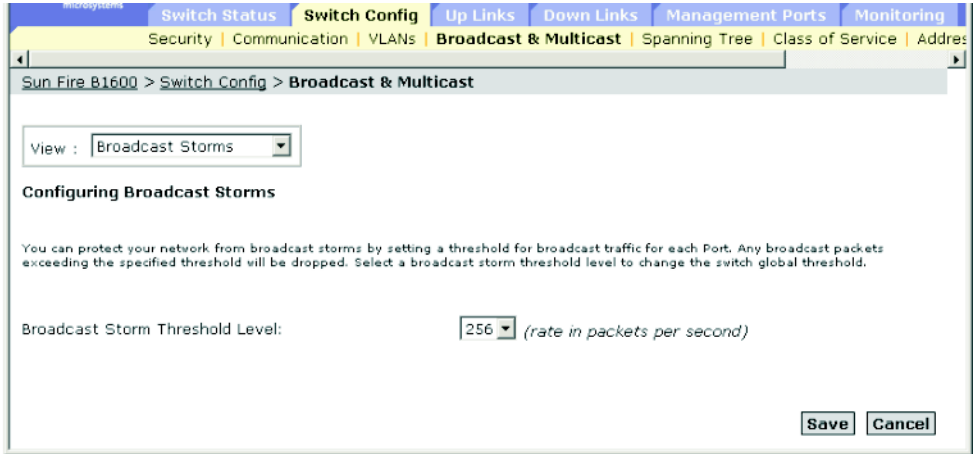
- Le contrôle des orages de diffusion est activé par défaut.
- Le contrôle de diffusion n'a aucun impact sur le trafic IP multidestinataire.

Attributs des commandes

- **Broadcast Storm Threshold Level*** : Seuil exprimé en paquets par seconde. (Plage : 16, 64, 128, 256 ; Par défaut : 256)

* L'ICL affiche « Broadcast Storm Limit ».

Web : Ouvrez Switch Config=>Broadcast & Multicast=>Broadcast Parameters. Définissez le niveau seuil, et cliquez sur Save.



ILC : Cet exemple affiche le seuil de diffusion défini à 64 paquets par seconde.

Remarque - Notez que la commande **switchport broadcast** active le contrôle des orages de diffusion sur l'interface spécifiée, et qu'elle définit le seuil de diffusion pour chaque interface du commutateur.

```
Console(config)#interface ethernet NETP7 4-74
Console(config-if)#switchport broadcast packet-rate 64 4-81
Console(config-if)#end
Console#show interfaces status ethernet NETP7 4-83
Information of NETP7
 Basic information:
  Port type: 1000T
  Mac address: 00-00-E8-66-66-83
 Configuration:
  Name: External RJ-45 connector NET7
  Port admin: Up
  Speed-duplex: Auto
  Capabilities: 10half, 10full, 100half, 100full, 1000full,
  Broadcast storm: Enabled
  Broadcast storm limit: 256 packets/second
  Flow control: Disabled
  Lacp: Disabled
 Current status:
  Link status: Up
  Port operation status: Up
  Operation speed-duplex: 1000full
  Flow control type: None
Console#
```

SNMP : Variables MIB équivalentes.

Nom de zone	Variable MIB	Accès	Plage de valeurs	Valeur par défaut
Broadcast Storm Packet Rate	sun... bcastStormMgt. bcastStormTable. bcastStormEntry. bcastStormPktRate	Lecture/ Ecriture	Nombre entier (16, 64, 128, 256)	256
Broadcast Storm Status	sun... bcastStormMgt. bcastStormTable. bcastStormEntry. bcastStormStatus	Lecture/ Ecriture	enabled (1), disabled (2)	enabled

3.3.4 Configuration de l'algorithme Spanning Tree

L'algorithme Spanning Tree (STA) peut être utilisé pour détecter et désactiver les boucles réseau et pour fournir des liaisons de sauvegarde entre les commutateurs, les ponts ou les routeurs. Ceci permet au commutateur d'interagir avec d'autres périphériques-ponts (à savoir un commutateur compatible STA, un pont ou un routeur) dans votre réseau pour garantir qu'une seule route existe entre deux stations du réseau et fournir des liaisons de sauvegarde qui remplacent automatiquement une liaison primaire désactivée.

Les algorithmes Spanning Tree pris en charge par ce commutateur comprennent les versions suivantes :

- STP : Protocole Spanning Tree (IEEE 802.1D)
- RSTP : Protocole Spanning Tree Rapide (IEEE 802.1w)

RSTP est destiné à remplacer le STP plus lent et datant des systèmes antérieurs. Le protocole RSTP permet une reconfiguration bien plus rapide (environ un dixième du temps requis par le STP) en réduisant le nombre de changements d'états requis avant que les ports actifs commencent l'apprentissage, en prédéfinissant un trajet alternatif qui peut être utilisé lorsqu'un noeud ou un port est défaillant et en conservant la base de données de transmission pour les ports insensibles aux changements dans l'arborescence quand la reconfiguration a lieu.

3.3.4.1 Configuration des paramètres STA de base

Les paramètres globaux s'appliquent à l'ensemble du commutateur.

Utilisation de la commande

- Protocole Spanning Tree Rapide

  Le RSTP prend en charge les connexions aux noeuds STP ou RSTP en surveillant les messages de protocole entrants et en modifiant de manière dynamique le type de messages de protocole transmis par le noeud RSTP tel que décrit ci-dessous :

  - Mode STP : Si le commutateur reçoit un BPDU 802.1D (à savoir un BPDU STP) après l'expiration du délai de migration d'un port, le commutateur suppose qu'il est connecté à un pont 802.1D et commence à n'utiliser que des BPDU 802.1D.
  - Mode RSTP : Si le RSTP utilise des BPDU 802.1D sur un port et reçoit un BPDU RSTP après l'expiration du délai de migration, le RSTP réinitialise l'horloge de migration et commence à utiliser des BPDU RSTP sur ce port.

Attributs de la commande

Configuration de base des paramètres globaux

Les attributs globaux suivants peuvent être configurés :

- **Enable Spanning Tree** : Active/désactive le STA sur le commutateur.
- **Spanning Tree Protocol** : Spécifie le type de Spanning Tree utilisé sur ce commutateur :
  - **STP** : Protocole Spanning Tree (IEEE 802.1D. En d'autres termes, quand cette option est sélectionnée, le commutateur utilise RSTP paramétré au mode de compatibilité STP forcée)
  - **RSTP** : Spanning Tree Rapide (IEEE 802.1w)

Les attributs globaux suivants sont fixes et ne peuvent pas être modifiés :

- **Bridge ID** : Priorité et adresse MAC de ce périphérique.
- **Designated Root** : Priorité et adresse MAC du périphérique du Spanning Tree que ce commutateur a accepté comme périphérique racine.
  - **Root Port** : Numéro du port du commutateur le plus proche de la racine. Ce commutateur communique avec le périphérique racine par le biais de ce port. S'il n'y a aucun port racine, le commutateur a été accepté en tant que périphérique racine du réseau Spanning Tree.
  - **Root Path Cost** : Distance entre le port racine du commutateur et le périphérique racine.
  - **Root Hello Time** : Intervalle (en secondes) auquel le périphérique transmet un message de configuration.
  - **Root Maximum Age** : Délai maximal (en secondes) pendant lequel ce périphérique peut attendre sans recevoir de message de configuration avant de tenter une reconfiguration. Tous les ports des périphériques (à l'exception des ports désignés) doivent recevoir des messages de configuration à intervalle régulier. Si le port racine élimine les informations STA (fournies dans le dernier message de configuration) pour cause d'obsolescence, un nouveau port racine est sélectionné parmi les ports de périphériques attachés au réseau. (Dans cette section, « ports » désignent les « interfaces », qui incluent à la fois les ports et les groupes.)
  - **Root Forward Delay** : Délai maximal (en secondes) pendant lequel le périphérique attend avant de passer d'un état à l'autre (à savoir, ignorer - apprendre - transmettre). Ce délai est nécessaire parce que chaque périphérique doit recevoir des informations sur les changements de topologie avant de commencer à transmettre les trames. En outre, chaque port a besoin de temps pour écouter les informations conflictuelles qui le renverraient à l'état « ignorer », sans quoi des boucles de données temporaires pourraient apparaître.
  - **Root Hold Time** : Intervalle (en secondes) pendant lequel deux unités de données du protocole de configuration de ponts au maximum sont transmises par ce noeud.

Configuration du périphérique racine

Les attributs globaux suivants peuvent être configurés :

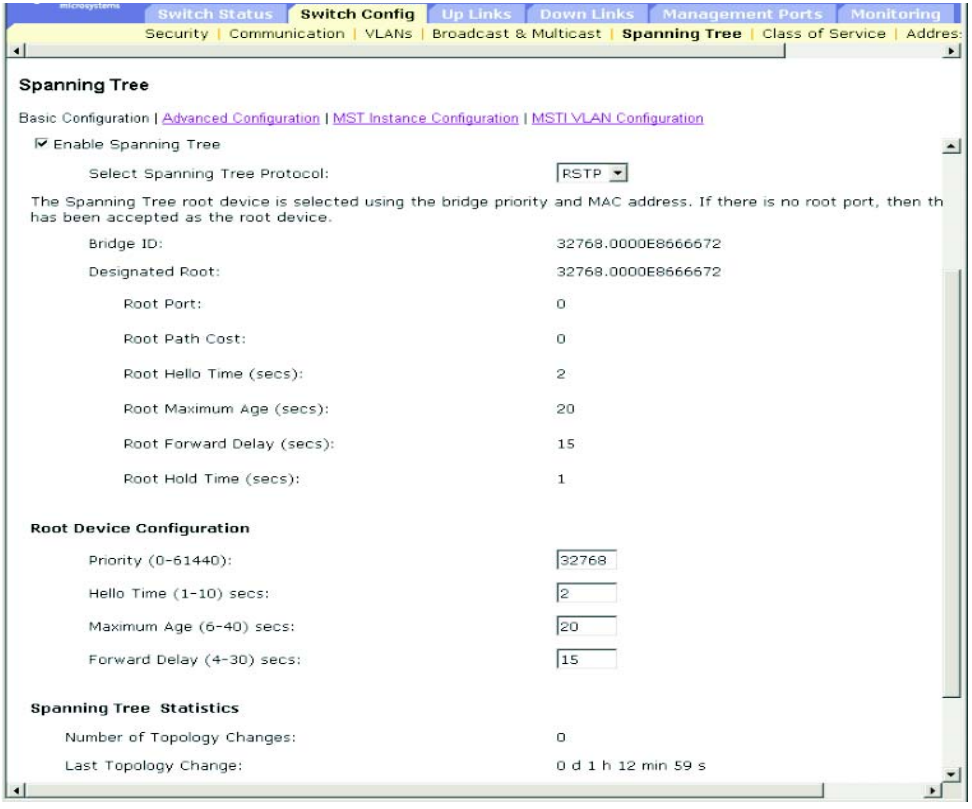
- **Priority** : La priorité du pont est utilisée pour sélectionner le périphérique racine, le port racine et le port désigné. Le périphérique avec la priorité la plus élevée devient le périphérique racine du STA. Toutefois, si tous les périphériques ont la même priorité, le périphérique racine est celui avec l'adresse MAC la moins élevée.
  - Valeurs par défaut : 32768
  - Plage : 0-61440, par incréments de 4096
  - Options : 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440
- **Hello Time** : Intervalle (en secondes) auquel le périphérique transmet un message de configuration.
  - Valeurs par défaut : 2
  - Minimum : 1
  - Maximum : Le plus bas de 10 ou [(Age max. du message / 2) -1]
- **Maximum Age** : Délai maximal (en secondes) pendant lequel ce périphérique peut attendre sans recevoir de messages de configuration avant de tenter une reconfiguration. Tous les ports des périphériques (à l'exception des ports désignés) doivent recevoir des messages de configuration à intervalle régulier. Le port qui élimine les informations STA fournies dans le dernier message de configuration reçu pour cause d'obsolescence devient le port désigné pour le LAN connecté. S'il s'agit d'un port racine, un nouveau port racine est sélectionné parmi les ports de périphériques connectés au réseau. (Dans cette section, « ports » signifie « interfaces », ce qui inclut à la fois les ports et les groupes.)
  - Valeurs par défaut : 20
  - Minimum : Le plus élevé de 6 ou [2 x (Hello Time + 1)].
  - Maximum : Le plus bas de 40 ou [2 x (Forward Delay -1)].
- **Forward Delay** : Délai maximal (en secondes) pendant lequel le périphérique attend avant de passer d'un état à l'autre (à savoir, ignorer - apprendre - transmettre). Ce délai est nécessaire parce que chaque périphérique doit recevoir des informations sur les changements de topologie avant de commencer à transmettre les trames. En outre, chaque port a besoin de temps pour écouter les informations conflictuelles qui le renverraient à l'état « ignorer », sans quoi des boucles de données temporaires pourraient apparaître.
  - Valeurs par défaut : 15
  - Minimum : Le plus élevé de 4 ou [(Age max. du message / 2) +1]
  - Maximum : 30

Statistiques du Spanning Tree

Les attributs globaux suivants affichent des valeurs statistiques et ne peuvent pas être modifiés :

- **Number of Topology Changes** : Nombre de reconfigurations du Spanning Tree.
- **Last Topology Change** : Temps écoulé depuis la dernière reconfiguration du Spanning Tree.

Web : Ouvrez Switch Config=>Spanning Tree=>Basic Configuration. Modifiez les attributs requis, puis cliquez sur Save.



Remarque - Si vous recevez un message d'erreur vous signalant que les données saisies ne sont pas valables, assurez-vous que les valeurs spécifiées pour Priority, Hello Time, Maximum Age et Forward Delay se situent dans la plage indiquée pour ces paramètres.

ILC : Cette commande affiche les paramètres STA globaux, suivis par les paramètres de chaque port.

```
Console#show spanning-tree4-103
Spanning-tree information
---------------------------------------------------------------
 Spanning tree mode               :RSTP
 Spanning tree enable/disable     :enable
 Priority                         :32768
 Bridge Hello Time (sec.)         :2
 Bridge Max Age (sec.)            :20
 Bridge Forward Delay (sec.)      :15
 Root Hello Time (sec.)           :2
 Root Max Age (sec.)              :20
 Root Forward Delay (sec.)        :15
 Designated Root                  :32768.0000E8666672
 Current root port                :0
 Current root cost                :0
 Number of topology changes       :0
 Last topology changes time (sec.):9142
 Transmission limit               :3
 Path Cost Method                 :4308020
.
.
.
```

Remarque - Le port racine courant ainsi que la distance racine courante indiquent zéro lorsque ce périphérique n'est pas connecté au réseau.

Cet exemple définit la valeur RSTP pour le mode Spanning Tree, active le Spanning Tree, puis définit les attributs indiqués.

```
Console(config)#spanning-tree mode rst4-94
Console(config)#spanning-tree4-93
Console(config)#spanning-tree priority 400004-97
Console(config)#spanning-tree hello-time 5                    4-96
Console(config)#spanning-tree max-age 404-96
Console(config)#spanning-tree forward-time 204-95
Console(config)#
```

SNMP : Variables MIB équivalentes.

Nom de zone	Variable MIB	Accès	Plage de valeurs	Valeur par défaut
STA System Status	sun...staMgt. staSystemStatus	Lecture/ Ecriture	enabled (1), disabled (2)	enabled
STA Protocol Type	sun...staMgt. staProtocolType	Lecture/ Ecriture	stp (1), rstp (2),	rstp
Bridge ID	Se compose de la priorité du pont et de l'adresse MAC.			
Designated Root	sun...xstMgt. mstInstanceCfgTable. mstInstanceCfgEntry. mstInstanceCfg-DesignatedRoot	Lecture seule	Chaîne d'octets	
Root Port	sun...xstMgt. mstInstanceCfgTable. mstInstanceCfgEntry. mstInstanceCfgRootPort	Lecture seule	Nombre entier	
Root Cost	sun...xstMgt. mstInstanceCfgTable. mstInstanceCfgEntry. mstInstanceCfgRootCost	Lecture seule	Nombre entier	
Hello Time	sun...staMgt.xstMgt. mstInstanceCfgTable. mstInstanceCfgEntry. mstInstanceCfg-HelloTime	Lecture seule	Nombre entier	200 centisecondes
Maximum Age	sun...staMgt.xstMgt. mstInstanceCfgTable. mstInstanceCfgEntry. mstInstanceCfgMaxAge	Lecture seule	Nombre entier	2000 centisecondes
Forward Delay	sun...staMgt.xstMgt. mstInstanceCfgTable. mstInstanceCfgEntry. mstInstanceCfg-ForwardDelay	Lecture seule	Nombre entier	1500 centisecondes
Priority	sun...staMgt.xstMgt. mstInstanceCfgTable. mstInstanceCfgEntry. mstInstanceCfgPriority	Lecture/ Ecriture	Nombre entier (0-61440)	32768
Bridge Hello Time	MIB-II. dot1dStp. dot1dStp-BridgeHelloTime	Lecture/ Ecriture	Nombre entier (100-1000) centisecondes	200 centisecondes

Nom de zone	Variable MIB	Accès	Plage de valeurs	Valeur par défaut
Bridge Maximum Age	MIB-II. dot1dStp. dot1dStpBridgeMaxAge	Lecture/ Ecriture	Nombre entier (600-4000) centisecondes	2000 centisecondes
Bridge Forward Delay	MIB-II. dot1dStp. dot1dStp-BridgeForwardDelay	Lecture/ Ecriture	Nombre entier (400-3000) centisecondes	1500 centisecondes
STA Configuration Changes	MIB-II. dot1dBridge.dot1dStp. dot1dStpTopChanges	Lecture seule	Compteur	
STA Last Topology Change	MIB-II. dot1dBridge.dot1dStp. dot1dStpTimeSince-TopologyChange	Lecture seule	Nombre entier	

3.3.4.2 Configuration des paramètres STA avancés

Cette section décrit les paramètres avancés du RSTP.

Attributs des commandes

- **Path Cost Method** : La distance à parcourir sert à déterminer le meilleur chemin entre les périphériques. Cette méthode permet de déterminer les plages de valeurs qui peuvent être affectées à chaque interface.
  - Long : Spécifie des valeurs 32 bits situées dans une fourchette de 1 à 200 000 000.
  - Short : Spécifie des valeurs 16 bits situées dans une fourchette de 1 à 65 535.
- **Transmission Limit** : Le taux de transmission maximum des BPDU est spécifié par la définition de l'intervalle minimal entre la transmission de messages de protocole consécutifs. (Plage : 1-10 ; Par défaut : 3)

Web : Ouvrez Switch Config=>Spanning Tree=>Advanced Configuration. Modifiez les attributs requis, puis cliquez sur Save.

Remarque - Si vous recevez un message d'erreur vous signalant que les données saisies ne sont pas valables, assurez-vous que vous avez spécifié une limite de transmission située dans la plage indiquée.

ILC : Cet exemple définit la méthode de détermination de la distance à parcourir du Spanning Tree ainsi que la limite de transmission.

```
Console(config)#spanning-tree pathcost method long4-98
Console(config)#spanning-tree transmission-limit 44-98
Console(config)#
```

SNMP : Variables MIB équivalentes.

Nom de zone	Variable MIB	Accès	Plage de valeurs	Valeur par défaut
RSTP Path Cost Method	sun... staMgt. staPathCostMethod	Lecture/ Ecriture	short (1), long (2)	long
RSTP Transmission Hold Count	sun.. staMgt. staTxHoldCount	Lecture/ Ecriture	Nombre entier (1-10)	3

3.3.5 Configuration de la classe des services

La classe de services (CdS) vous permet de spécifier les paquets de données prioritaires quand le trafic est placé dans le tampon du commutateur en raison d'une saturation du réseau. Le commutateur prend en charge les classes de service avec quatre files d'attente correspondant à différentes priorités pour chaque port. Les paquets de données se trouvant dans la file d'attente avec la priorité la plus élevée seront transmis avant ceux de la file d'attente avec la priorité la plus basse. Vous pouvez définir la priorité par défaut de chaque interface et configurer l'affectation de marques de priorité aux files d'attente du commutateur.

3.3.5.1 Définition de la priorité par défaut des interfaces

Vous pouvez spécifier la priorité du port par défaut pour chaque interface sur le commutateur. Tous les paquets non marqués entrant dans le commutateur reçoivent la marque correspondant à la priorité du port par défaut spécifié, puis sont placés dans les files d'attente appropriées sur le port de sortie.

Utilisation de la commande

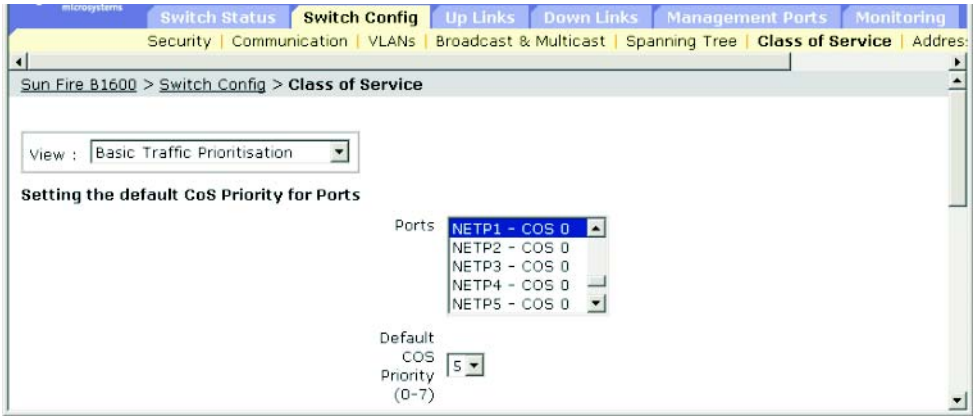
- Ce commutateur propose quatre files d'attente correspondant à différentes priorités sur chaque port. Il utilise un protocole WRR (Weighted Round Robin) pour empêcher un blocage au début de la file d'attente.
- La priorité par défaut s'applique à une trame non marquée reçue sur un port paramétré pour accepter tous les types de trames (en d'autres termes, il reçoit les trames marquées et non marquées). Cette priorité ne s'applique pas aux trames marquées VLAN IEEE 802.1Q. Si la trame entrante est une trame marquée VLAN IEEE 802.1Q, les bits Priorité utilisateur IEEE 802.1p seront utilisés.
- Si le port de sortie est un membre non marqué du VLAN associé, toutes les marques VLAN sont supprimées de ces trames avant leur transmission.

Attributs des commandes

- **Ports :** Interface (port ou groupe) et priorité CdS affectée par défaut.
- **Default COS Priority*** : Priorité affectée aux trames non marquées reçues sur l'interface spécifiée. (Plage : 0-7 ; Par défaut : 0)

* L'ILC affiche ces informations sous la forme « Priority for untagged traffic ».

Web : Ouvrez Switch Config=>Class of Service=>Basic Traffic Prioritisation. Faites défiler jusqu'à « Setting the Default CoS Priority for Ports ». Sélectionnez une interface dans la liste Ports, modifiez la priorité par défaut, puis cliquez sur Save.



ILC : Cet exemple affecte une priorité par défaut de 5 au port NETP1.

```
Console(config)#interface ethernet NETP1 4-74
Console(config-if)#switchport priority default 5                4-133
Console#show interfaces switchport ethernet NETP1 4-85
Information of NETP1
 Broadcast threshold: Enabled, 256 packets/second
 Lacp status: Disabled
 VLAN membership mode: Hybrid
 Ingress rule: Disabled
 Acceptable frame type: All frames
 Native VLAN: 1
 Priority for untagged traffic: 5
 Gvrp status: Enabled
 Allowed Vlan:    1(u),
 Forbidden Vlan:
Console#
```

SNMP : Variables MIB équivalentes.

Nom de zone	Variable MIB	Accès	Plage de valeurs	Valeur par défaut
Port Default User Priority	MIB-II. dot1dBridge. pBridgeMIB. pBridgeMIBObjects. dot1dPriority. dot1dPortPriorityTable. dot1dPortPriorityEntry. dot1dPortDefault-UserPriority	Lecture/ Ecriture	Nombre entier (0-7)	0

3.3.5.2 Affectation de valeurs CdS aux files d'attente de sortie

Le commutateur traite le trafic contenant des marques de priorité des classes de service (CdS) à l'aide des quatre files d'attente de chaque port, avec des échéanciers de service basés sur le protocole WRR (Weighted Round Robin) (page 4-70). Jusqu'à 8 priorités de trafic distinctes sont définies dans IEEE 802.1p. Les niveaux de priorité par défaut sont affectés conformément aux recommandations de la norme IEEE 802.1p, telles que présentées dans le tableau suivant.

	File d'attente			
Priorité	0	1	2	3
		0		
	1			
	2			
		3		
			4	
			5	
				6
				7

Les niveaux de priorité recommandés dans la norme IEEE 802.1p pour les différentes applications réseau sont indiqués dans le tableau suivant. Toutefois, vous pouvez affecter aux files d'attente de sortie du commutateur les niveaux de priorité convenant le mieux au trafic applicatif de votre propre réseau.

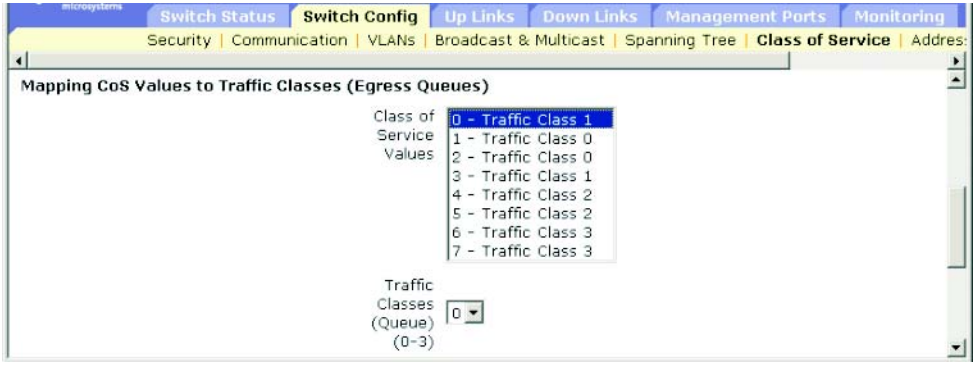
Niveau de priorité	Type de trafic
1	Contexte
2	(Libre)
0 (par défaut)	Best Effort
3	Excellent Effort
4	Controlled Load
5	Vidéo, moins de 100 millisecondes de latence et de perturbations
6	Audio, moins de 10 millisecondes de latence et de perturbation
7	Network Control

Attributs des commandes

- **Class of Service Values** : Valeur CdS. (Plage : 0-7 ; 7 étant la priorité la plus élevée)
- **Traffic Classes (Queue)*** : Tampon de la file d'attente de sortie (Plage : 0-3)

* L'ILC affiche l'identificateur de la file d'attente.

Web : Ouvrez Switch Config=>Class of Service=>Basic Traffic Prioritisation. Faites défiler jusqu'à Mapping CoS Values to Traffic Classes (Egress Queues). Sélectionnez une priorité dans la liste Class of Service Values, sélectionnez une file d'attente de sortie dans la liste déroulante Traffic Classes, puis cliquez sur Save.



ILC : L'exemple suivant montre comment affecter les valeurs CdS 0, 1 et 2 à la file d'attente avec priorité CdS 0, la valeur 3 à la file d'attente avec priorité CdS 1, les valeurs 4 et 5 à la file d'attente avec priorité CdS 2, et les valeurs 6 et 7 à la file d'attente avec priorité CdS 3.

```
Console(config)#interface ethernet NETP04-74
Console(config)#queue cos-map 0 0 1 24-135
Console(config)#queue cos-map 1 3
Console(config)#queue cos-map 2 4 5
Console(config)#queue cos-map 3 6 7
Console(config)#exit
Console#show queue cos-map ethernet NETP04-137
Information of NETP0
 Queue ID  Class of service
 --------  ----------------
    0      0 1 2
    1      3
    2      4 5
    3      6 7
Console#
```

SNMP : Variables MIB équivalentes.

Nom de zone	Variable MIB	Accès	Plage de valeurs	Valeur par défaut
Traffic Class Priority	MIB-II. dot1dBridge. pBridgeMIB. pBridgeMIBObjects. dot1dPriority. dot1dTrafficClassTable. dot1dTrafficClassEntry. dot1dTrafficClassPriority	Non accessible	Nombre entier (0-7)	
Traffic Class	MIB-II. dot1dBridge. pBridgeMIB. pBridgeMIBObjects. dot1dPriority. dot1dTrafficClassTable. dot1dTrafficClassEntry. dot1dTrafficClass	Lecture/ Ecriture	Nombre entier (0-7)	page 4-67

3.3.5.3 Configuration du poids des services pour les classes de trafic

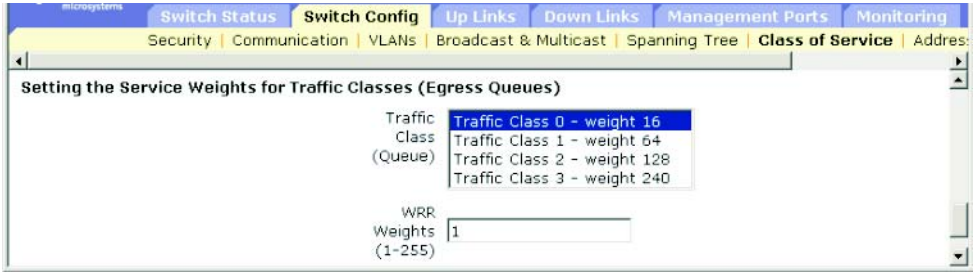
Ce commutateur utilise l'algorithme WRR (Weighted Round Robin) pour déterminer la fréquence à laquelle il traite chaque file d'attente. Comme décrit dans « Affectation de valeurs CdS aux files d'attente de sortie » à la page 3-67, les classes de trafic sont affectées à l'une des quatre files d'attente de sortie proposées sur chaque port. Vous pouvez affecter un poids à chacune de ces files d'attente (et, par conséquent, les priorités de trafic correspondantes). Ce poids définit la fréquence à laquelle chaque file d'attente est interrogée pour traitement, puis affecte les temps de réponse des applications logicielles avec une valeur de priorité spécifique.

Attributs des commandes

- **Traffic Class (Queue)*** : Affiche une liste des poids pour chaque classe de trafic.
- **WRR Weights** : Définit un nouveau poids pour la classe de trafic sélectionnée. (Plage : 1-255)

* L'ILC affiche l'identificateur de la file d'attente.

Web : Ouvrez Switch Config=>Class of Service=>Basic Traffic Prioritisation. Faites défiler jusqu'à Setting the Service Weights for Traffic Classes (Egress Queues). Sélectionnez une classe de trafic (à savoir une file d'attente de sortie), entrez un poids, puis cliquez sur Save.



ILC : L'exemple suivant montre comment affecter des poids WRR de 1, 4, 16 et 64 aux files d'attente de priorité CdS 0, 1, 2 et 3.

```
Console(config)#queue bandwidth 1 4 16 64 4-134
Console(config)#exit
Console#show queue bandwidth 4-136
 Queue ID Weight
 -------- ------
        0      1
        1      4
        2     16
        3     64
Console#
```

SNMP : Variables MIB équivalentes.

Nom de zone	Variable MIB	Accès	Plage de valeurs	Valeur par défaut
WRR Traffic Class (Queue ID)	sun... priorityMgt. prioWrrTable. prioWrrEntry. prioWrrTrafficClass	Index	Nombre entier (0-7)	
WRR Weight	sun... priorityMgt. prioWrrTable. prioWrrEntry. prioWrrWeight	Lecture/ Ecriture	Nombre entier (1-255)	Pour la file d'attente 0 : 16 Pour la file d'attente 1 : 64 Pour la file d'attente 2 : 128 Pour la file d'attente 3 : 240

3.3.5.4 Affectation de priorités de couche 3/4 aux valeurs CdS

Ce commutateur prend en charge plusieurs méthodes communes de priorisation du trafic de la couche 3/4 pour répondre aux exigences des applications. Les priorités de trafic peuvent être spécifiées dans l'en-tête IP d'une trame, à l'aide des bits de priorité de l'octet Type de Service (TdS). Si vous avez recours aux bits de priorité, l'octet TdS peut contenir trois bits pour la priorité IP ou six pour les services DSCP (Differentiated Services Code Point). Lorsque ces services sont activés, les priorités sont affectées à une valeur CdS par le commutateur, et le trafic alors envoyé à la file d'attente de sortie correspondante.

Etant donné que le trafic peut contenir différentes informations de priorité, ce commutateur affecte des valeurs de priorité aux files d'attente de sortie de la manière suivante :

- L'ordre d'affectation des priorités est Priorité IP ou Priorité DSCP, puis Priorité du port par défaut.
- La priorité IP et la priorité DSCP ne peuvent pas être activées toutes les deux. L'activation de l'une d'entre elles désactive automatiquement l'autre.

Attributs des commandes

- **Enable Priority Services :** Vous pouvez activer ou désactiver l'affectation des priorités de la couche 3/4 aux valeurs CdS. (Par défaut : désactivée)
- **IP Precedence** : Affecte les priorités de la couche 3/4 à l'aide de la priorité IP.
- **Differentiated Services Code Point Mapping (DSCP)** : Affecte les priorités de la couche 3/4 à l'aide du DSCP.

Web : Ouvrez Switch Config=>Class of Service=>Layer 3/4 Traffic Prioritisation. Marquez Enable Priority Services, sélectionnez IP Precedence ou DSCP, et cliquez sur Save.

ILC : L'exemple suivant active le service IP Precedence sur le commutateur.

```
Console(config)#map ip precedence4-137
Console(config)#
```

Pour désactiver complètement la priorisation du trafic sur la couche 3/4, utilisez les commandes suivantes.

```
Console(config)#no map ip precedence4-137
Console(config)#no map ip dscp4-139
```

SNMP : Variables MIB équivalentes.

Nom de zone	Variable MIB	Accès	Plage de valeurs	Valeur par défaut
IP Precedence/ DSCP Status	sun... priorityMgt. prioIpPrecDscpStatus	Lecture/ Ecriture	disabled (1) precedence (2), dscp (3)	disabled

3.3.5.5 Affectation des priorités IP

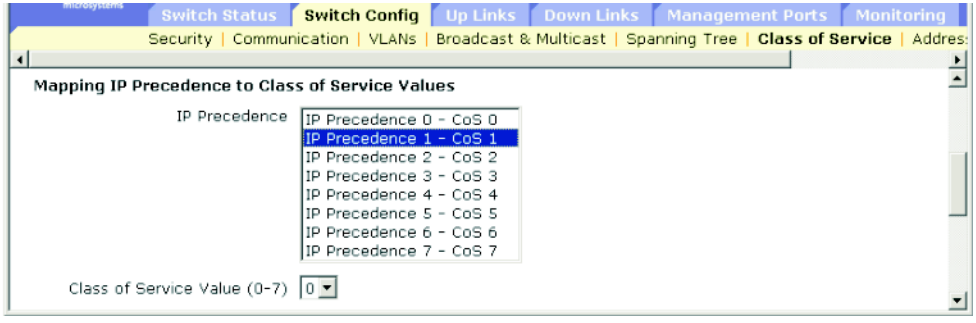
L'octet Type de Service (TdS) de l'en-tête IPv4 inclut trois bits de priorité définissant huit niveaux de priorité différents allant de la priorité la plus élevée pour les paquets soumis au contrôle réseau à la priorité la plus faible pour le trafic de routine. Les valeurs de la priorité IP par défaut sont affectées sur une base univoque aux valeurs CdS (ainsi, la valeur de priorité IP 0 est affectée à la valeur CdS 0, etc). Les bits 6 et 7 sont utilisés pour le contrôle réseau, et les autres bits pour différents types d'application. Les bits TdS sont définis dans le tableau suivant.

Niveau de priorité	Type de trafic
7	Contrôle réseau
6	Contrôle Interréseau
5	Critique
4	Ignorer Flash
3	Flash
2	Immédiat
1	Priorité
0	Routine

Attributs des commandes

- **IP Precedence** : Affiche l'affectation des priorités IP aux valeurs CdS.
- **Class of Service Value :** Affecte une valeur CdS à la valeur de priorité IP sélectionnée. Notez que « 0 » représente une priorité faible et « 7 » une priorité élevée.

Web : Ouvrez Switch Config=>Class of Service=>Layer 3/4 Traffic Prioritisation. Faites défiler jusqu'à Mapping IP Precedence to Class of Service Values. Sélectionnez une entrée dans la table IP Precedence, entrez une valeur dans la zone Class of Service Value, puis cliquez sur Save.



ILC : L'exemple suivant affecte la valeur de priorité IP 1 à la valeur CdS 0 sur le port SNP5*, puis affiche tous les paramètres de priorité IP pour ce port.

```
Console(config)#interface ethernet SNP5 4-74
Console(config-if)#map ip precedence 1 cos 0                    4-138
Console(config-if)#end
Console#show map ip precedence ethernet SNP5 4-141
Precedence mapping status: disabled

 Port      Precedence COS
 --------- ---------- ---
      SNP5          0   0
      SNP5          1   0
      SNP5          2   2
      SNP5          3   3
      SNP5          4   4
      SNP5          5   5
      SNP5          6   6
      SNP5          7   7
Console#
```

* L'affectation de valeurs spécifiques pour la priorité IP est mise en oeuvre sous la forme d'une commande de configuration d'interface, mais toute modification s'applique à toutes les interfaces du commutateur.

SNMP : Variables MIB équivalentes.

Nom de zone	Variable MIB	Accès	Plage de valeurs	Valeur par défaut
IP Precedence Value	sun... priorityMgt. prioIpPrecTable. prioIpPrecEntry. prioIpPrecValue	Non accessible	Nombre entier (0-7)	
IP Precedence CoS	sun... priorityMgt. prioIpPrecTable. prioIpPrecEntry. prioIpPrecCos	Lecture/ Ecriture	Nombre entier (0-7)	Affectation univoque

3.3.5.6 Affectation des priorités DSCP

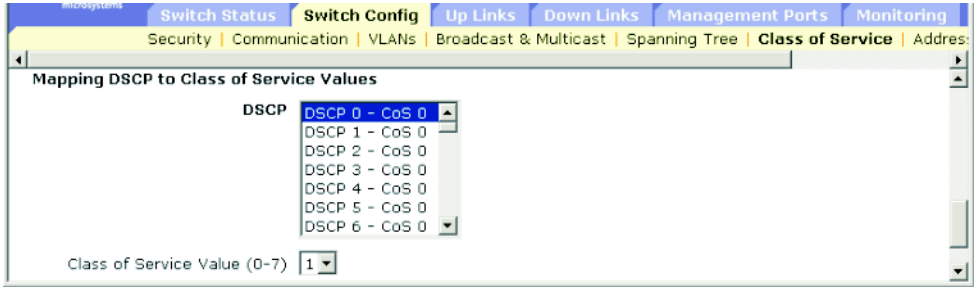
Le DSCP comporte six bits, permettant de coder jusqu'à 64 comportements de transmission différents. Le DSCP remplace les bits ToS, mais reste compatible avec les trois bits de priorité de telle sorte que les périphériques non compatibles DSCP, les périphériques TdS, n'entrent pas en conflit avec l'affectation DSCP. Sur la base des politiques du réseau, plusieurs types de trafic peuvent être marqués pour différents types de transmission. Les valeurs DSCP par défaut sont définies dans la table suivante. Remarquez que toutes les valeurs DSCP qui ne sont pas spécifiées dans la table suivante sont affectées à la valeur CdS 0.

Valeur IP DSCP	Valeur CdS
0	0
8	1
10, 12, 14, 16	2
18, 20, 22, 24	3
26, 28, 30, 32, 34, 36	4
38, 40, 42	5
48	6
46, 56	7

Attributs des commandes

- **DSCP** : Affiche l'affectation des priorités DSCP aux valeurs CdS.
- **Class of Service Value** : Affecte une valeur CdS à la valeur de priorité DSCP sélectionnée. Notez que « 0 » représente une priorité faible et « 7 » une priorité élevée.

Web : Ouvrez Switch Config=>Class of Service=>Layer 3/4 Traffic Prioritisation. Faites défiler jusqu'à Mapping DSCP to Class of Service Values. Sélectionnez une entrée dans la table DSCP, entrez une valeur dans la zone Class of Service Value, puis cliquez sur Save.



ILC : L'exemple suivant affecte la valeur DSCP 0 à la valeur CdS 1 sur le port SNP5*, puis affiche tous les paramètres DSCP Priority pour ce port.

```
Console(config)#interface ethernet SNP5 4-74
Console(config-if)#map ip dscp 0 cos 1 4-140
Console(config-if)#end
Console#show map ip dscp ethernet SNP5 4-142
DSCP mapping status: disabled

 Port        DSCP COS
 ----------- ---- ---
        SNP1    0   1
        SNP1    1   0
        SNP1    2   0
        SNP1    3   0
.
.
.
        SNP1    61   0
        SNP1    62   0
        SNP1    63   0
Console#
```

* L'affectation de valeurs spécifiques pour IP DSCP est mise en oeuvre sous la forme d'une commande de configuration d'interface, mais toute modification s'applique à toutes les interfaces du commutateur.

SNMP : Variables MIB équivalentes.

Nom de zone	Variable MIB	Accès	Plage de valeurs	Valeur par défaut
IP DSCP Value	sun... priorityMgt. prioIpDscpTable. prioIpDscpEntry. prioIpDscpValue	Non accessible	Nombre entier (0-63)	
IP DSCP CoS	sun... priorityMgt. prioIpDscpTable. prioIpDscpEntry. prioIpDscpCos	Lecture/ Ecriture	Nombre entier (0-7)	Page 4-75

3.3.6 Paramètres de la table d'adressage

Les commutateurs enregistrent les adresses de tous les périphériques connus. Ces informations servent à assurer le routage du trafic directement entre les ports d'entrée et de sortie. Toutes les adresses apprises par la surveillance du trafic sont stockées dans la table d'adressage dynamique. Vous pouvez également configurer manuellement les adresses statiques liées à un port spécifique.

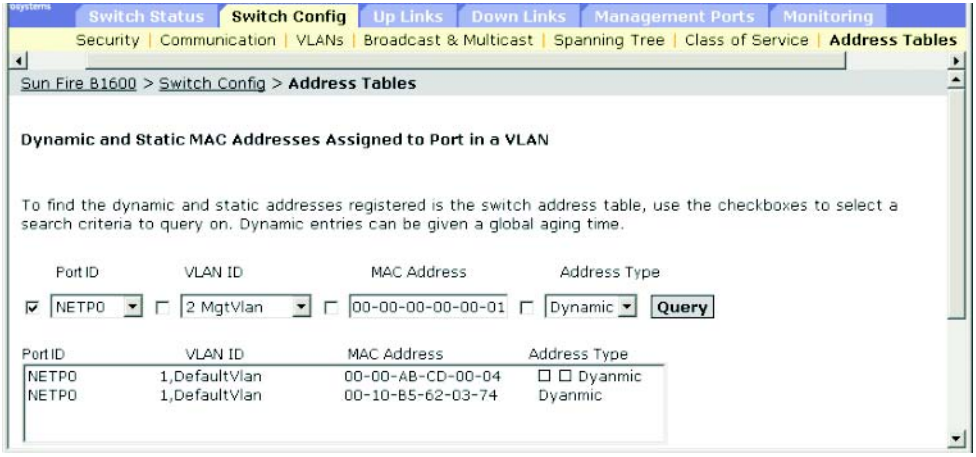
3.3.6.1 Affichage de la table d'adressage

La table d'adressage contient les adresses MAC apprises de manière dynamique par la surveillance de l'adresse source pour le trafic entrant dans le commutateur. Lorsque l'adresse de destination du trafic entrant se trouve dans la base de données, les paquets qui lui sont destinés sont transmis directement au port associé. Sinon, le trafic est transmis à tous les ports. La table d'adressage inclut également les adresses MAC statiques liées à un port spécifique. (Reportez-vous à la section « Configuration d'adresses statiques » à la page 3-100).

Attributs des commandes

- **Port ID** (Interface*) : Port ou groupe (ports à liaison ascendante : NETP0-7 ; ports à liaison descendante : SNP0-15 ; vous ne pouvez pas afficher la table d'adressage MAC pour NETMGT).
- **VLAN ID** : Identificateur du VLAN (1-4094). (Ce champ contient l'identificateur du VLAN et son nom).
- **MAC Address** : Adresse MAC associée à cette interface.
- **Address Type** : Indique si l'adresse a été apprise ou configurée de manière statique.

Web : Ouvrez Switch Config=>Security. Spécifiez une interface, un VLAN, une adresse MAC ou un type d'adresse (ou toute combinaison de ceux-ci) pour les critères de recherche, puis cliquez sur Query.



ILC : Cet exemple affiche les entrées de la table d'adressage pour le port NETP1.

```
Console#show mac-address-table interface ethernet NETP14-88
 Interface   Mac Address       Vlan Type
 ----------- ----------------- ---- -----------------
       NETP0 00-20-9c-23-cd-61 1    Dynamic
Console#
```

SNMP : Variables MIB équivalentes.

Nom de zone	Variable MIB	Accès	Plage de valeurs
Interface	MIB-II. dot1dBridge.dot1dTp. dot1dTpFdbTable.dot1dTpFdbEntry. dot1dTpFdbPort	Lecture seule	not learned (0), Port List (1-24)
MAC Address	MIB-II. dot1dBridge.dot1dTp. dot1dTpFdbTable.dot1dTpFdbEntry. dot1dTpFdbAddress	Lecture seule	Adresse MAC
VLAN	MIB-II. dot1dBridge.qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanStaticTable. dot1qVlanStaticEntry. dot1qVlanIndex	Non accessible	Nombre entier
Type	MIB-II. dot1dBridge.dot1dTp. dot1dTpFdbTable.dot1dTpFdbEntry. dot1dTpFdbStatus	Lecture seule	other (1), invalid (2) learned (3), self (4), mgmt (5)

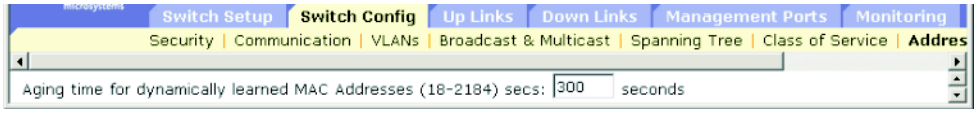
3.3.6.2 Modification du délai d'obsolescence

Vous pouvez définir un délai d'obsolescence pour les entrées de la table d'adressage dynamique.

Attributs des commandes

- **Aging Time** : Délai après lequel une entrée apprise est ignorée. (Plage : 18-2184 secondes ; Par défaut : 300 secondes)

Web : Cliquez sur Switch Config=>Address Tables. Spécifiez le nouveau délai d'obsolescence, puis cliquez sur Save.



ILC : Cet exemple définit le délai d'obsolescence à 400 secondes.

```
Console(config)#mac-address-table aging-time 400
Console(config)#
```

4-89

SNMP : Variables MIB équivalentes.

Nom de zone	Variable MIB	Accès	Plage de valeurs	Valeur par défaut
Aging Time	MIB-II. dot1dBridge.dot1dTp. dot1dTpAgingTime	Lecture/ Ecriture	Nombre entier (18-2184) secondes	300 secondes

3.4 Configuration du port

Cette section comprend les menus de configuration des ports à liaison descendante, des ports à liaison ascendante et du port de gestion. La plupart de ces menus s'appliquent à tous les types de port. Toutefois, le port de gestion ne prend en charge que quelques menus de base, et le filtrage des paquets (page 4-111) n'est prévu que pour le port de gestion.

Remarque - Les désignations des ports utilisées dans les menus suivants sont NETP0-7 pour les ports à liaison ascendante-, SNP0-15 pour les ports à liaison descendante et NETMGT pour le port de gestion.

3.4.1 Affichage de l'état de la connexion

Vous pouvez utiliser la page Port Status pour afficher l'état de la connexion courante, y compris l'état du lien, le mode speed/duplex, le contrôle de flux, l'auto-négociation et le contrôle des orages de diffusion.

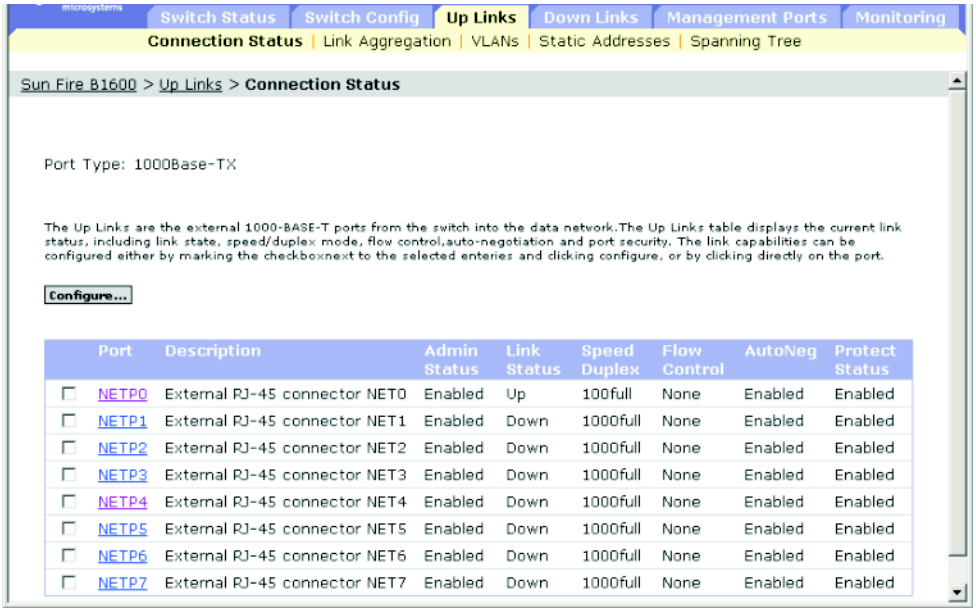
Attributs des commandes

- **Port Type :** Indique le type de port (1000Base-SX, 1000Base-T ou 10/100Base-TX).
- **Port** : Port ou groupe (ports à liaison ascendante : NETP0-7, ports à liaison descendante : SNP0-15, port de gestion : NETMGT).
- **Description :** étiquette de l'interface.
- **Admin Status :** Indique si l'interface est activée ou désactivée.
  Web : Affiche Enabled ou Disabled.
  ILC : Affiche l'admin du port (ascendant ou descendant).
- **Link Status :** Indique si la liaison est ascendante ou descendante.
- **Port Operation Status** : Fournit des informations détaillées sur l'état du port. ILC uniquement ; n'affiche cet élément que si la liaison est ascendante.
- **Speed/Duplex :** Affiche la vitesse courante ainsi que le mode duplex.
- **Flow Control :** Indique si le contrôle de flux est activé ou désactivé.
  Web : IEEE 802.3x, Back-Pressure ou None.
  ILC : Enabled ou Disabled. Le type de flux affiche IEEE 802.3x, Back-Pressure ou None.
- **Auto-negotiation** : Indique si l'auto-négociation est activée ou désactivée.
- **Protect Status** : Indique si le contrôle des orages de diffusion a été activé ou non sur cette interface. Pour définir la valeur seuil, reportez-vous à « Contrôle des orages de diffusion (Global Setting) » à la page 3-55.

- **MAC Address** : Adresse de ce port sur la couche physique. ILC uniquement ; pour accéder à cet élément sur le Web, reportez-vous à « Définition de l'adresse IP » à la page 3-11.
- **Port Capabilities*** **:** Indique les capacités à publier pour un port pendant l'auto-négociation. Les capacités suivantes sont prises en charge.
  - **10half** : Prend en charge le fonctionnement en semi duplex à 10 Mbps
  - **10full** : Prend en charge le fonctionnement en duplex à 10 Mbps
  - **100half** : Prend en charge le fonctionnement en semi duplex à 100 Mbps
  - **100full** : Prend en charge le fonctionnement en duplex à 100 Mbps
  - **1000full** : Prend en charge le fonctionnement en duplex à 1000 Mbps
  - **Sym :** Transmet et reçoit les trames de pause pour le contrôle du flux
  - **FC** : Prend en charge le contrôle de flux
- **LACP Status** : Indique si le protocole LACP (Link Aggregation Control Protocol) a été activé sur ce port. (ILC uniquement)

* Pour accéder à cet élément sur le Web, reportez-vous à « Configuration des connexions d'interface » à la page 3-84.

Web : Cliquez sur Up Links / Down Links / Management Port=>Status. Pour configurer les connexions d'une ou plusieurs interfaces, cliquez sur la case à cocher située en regard des entrées sélectionnées et cliquez sur Configure. (Reportez-vous à la section « Configuration des connexions d'interface » à la page 3-84).



ILC : Cet exemple affiche l'état de la connexion du port NETP7.

```
Console#show interfaces status ethernet NETP7
Information of NETP7
 Basic information:
  Port type: 1000T
  Mac address: 00-00-E8-66-66-83
 Configuration:
  Name: External RJ-45 connector NET7
  Port admin: Up
  Speed-duplex: Auto
  Capabilities: 10half, 10full, 100half, 100full, 1000full,
  Broadcast storm: Enabled
  Broadcast storm limit: 256 packets/second
  Flow control: Disabled
  Lacp: Disabled
 Current status:
  Link status: Up
  Port operation status: Up
  Operation speed-duplex: 1000full
  Flow control type: None
Console#
```

4-83

SNMP : Variables MIB équivalentes.

Nom de zone	Variable MIB	Accès	Plage de valeurs	Valeur par défaut
Port Type	sun... portMgt. portTable portEntry. portType	Lecture seule	other(1), hundredBaseTX(2), hundredBaseFX(3), thousandBaseSX(4), thousandBaseLX(5), thousandBaseT(6), thousandBaseMiniGBIC(7) thousandBaseSFP(8)	
MAC Address	MIB-II. interfaces. ifTable.ifEntry. ifPhysAddress	Lecture seule	Adresse physique	
Port	sun... portMgt. portTable portEntry.	Index	Nombre entier (1-25)	

Nom de zone	Variable MIB	Accès	Plage de valeurs	Valeur par défaut
Port Name	sun... portMgt. portTable portEntry. portName	Lecture/ Ecriture	Chaîne d'affichage (Taille (0-64))	
Administrative Status	MIB-II. interfaces. ifTable.ifEntry. ifAdminStatus	Lecture/ Ecriture	up (1), down (2), testing (3)	up
Link Status	MIB-II. interfaces. ifTable.ifEntry. ifOperStatus	Lecture seule	up (1), down (2-7),	
Operational Status	MIB-II. interfaces. ifTable.ifEntry. ifOperStatus	Lecture seule	up (1), down (2), testing (3) unknown (4), dormant (5), notPresent (6), lowerLayerDown (7)	
Port Speed Duplex Status	sun... portMgt. portTable.portEntry. portSpeedDpxStatus	Lecture seule	error(1), halfDuplex10(2), halfDuplex10(3), halfDuplex100(4), fullDuplex100(5), halfDuplex1000(6), fullDuplex1000(7)	
Port Capabilities	sun... portMgt. portTable.portEntry. portCapabilities	Lecture/ Ecriture	Bits{ portCap10half (0), portCap10full (1), portCap100half (2), portCap100full (3), portCap1000half (4), portCap1000full (5), reserved6-13 (6-13), portCapSym (14), portCapFlowCtrl (15)}	
Port Flow Control Status	sun... portMgt. portTable.portEntry. portFlowCtrlStatus	Lecture seule	error(1), backPressure(2), dot3xFlowControl(3), none(4)	none

Nom de zone	Variable MIB	Accès	Plage de valeurs	Valeur par défaut
LACP Port Status	sun... lacpMgt. lacpPortTable. lacpPortEntry. lacpPortStatus	Lecture/ Ecriture	enabled (1), disabled (2)	disabled
Port Auto-negotiation	sun... portMgt. portTable.portEntry. portAutonegotiation	Lecture/ Ecriture	enabled (1), disabled (2)	enabled
Broadcast Storm Status	sun... bcastStormMgt. bcastStormTable. bcastStormEntry. bcastStormStatus	Lecture/ Ecriture	enabled (1), disabled (2)	enabled

3.4.2 Configuration des connexions d'interface

Vous pouvez utiliser la page Port Setup pour activer/désactiver une interface, définir l'auto-négociation et les capacités d'interface à publier ou encore pour régler manuellement la vitesse, le mode duplex et le contrôle de flux.

Attributs des commandes

- **Port/s** : Port ou groupe (liaisons ascendantes : NETP0-7, liaisons descendantes : SNP0-15).
- **Port Description :** Vous permet d'étiqueter une interface. (Plage : 1-64 caractères ; Par défaut : liaisons ascendantes : Connecteur RJ-45 externe NETn, liaisons descendantes : Emplacement du serveur Blade n ; port de gestion : connecteur RJ-45 externe NETMGT)
- **Administrative Status :** Vous permet de désactiver manuellement une interface. Vous pouvez désactiver une interface en raison d'un comportement anormal (p.ex. collisions excessives), puis la réactiver une fois le problème résolu. Vous pouvez également désactiver une interface à des fins de sécurité.
- **Negotiate Link Capabilities**[1] **:** Permet d'activer/désactiver l'auto-négociation. Lorsque l'auto-négociation est activée, vous devez spécifier les capacités à publier. Lorsque l'auto-négociation est désactivée, vous pouvez forcer les paramètres de vitesse, mode et contrôle de flux. Les capacités suivantes sont prises en charge.
  - **10half** : Prend en charge le fonctionnement en semi duplex à 10 Mbps
  - **10full** : Prend en charge le fonctionnement en duplex à 10 Mbps
  - **100half** : Prend en charge le fonctionnement en semi duplex à 100 Mbps
  - **100full** : Prend en charge le fonctionnement en duplex à 100 Mbps
  - **1000half** : Prend en charge le fonctionnement en semi duplex à 1000 Mbps

- **1000full** : Prend en charge le fonctionnement en duplex à 1000 Mbps
- **symmetric** (Gigabit only) : Cochez cette option pour transmettre et recevoir des trames de pause ou décochez-la pour activer l'auto-négociation de l'émetteur et du récepteur pour les trames de pause asymétriques. (Le commutateur ne prend en charge que les trames de pause symétriques.)
- **flowcontrol** : Prend en charge le contrôle de flux
  Le contrôle de flux peut éliminer la perte de trames en « bloquant » le trafic depuis les stations ou les segments terminaux connectés directement au commutateur lorsque son tampon se remplit. En cas d'activation, la contre-pression est utilisée pour le fonctionnement en semi duplex et IEEE 802.3x pour un fonctionnement en duplex.

Remarque - Les commutateurs intégrés sur le châssis Sun Fire™ B1600 pour serveurs Blade sont chacun composés de deux puces de commutateurs reliées. Il n'est possible d'activer le contrôle de flux qu'entre deux ports de la même puce de commutateur. Les ports NETP0, NETP1, NETP4, NETP5 ainsi que SNP8 à SNP15 se trouvent sur l'une des puces. Les ports NETP2, NETP3, NETP6, NETP7 ainsi que SNP0 à SNP7 se trouvent sur l'autre. Si vous regardez le panneau arrière de l'unité commutateur/contrôleur système, tous les ports de droite se trouvent sur une puce et tous ceux de gauche sur l'autre.)

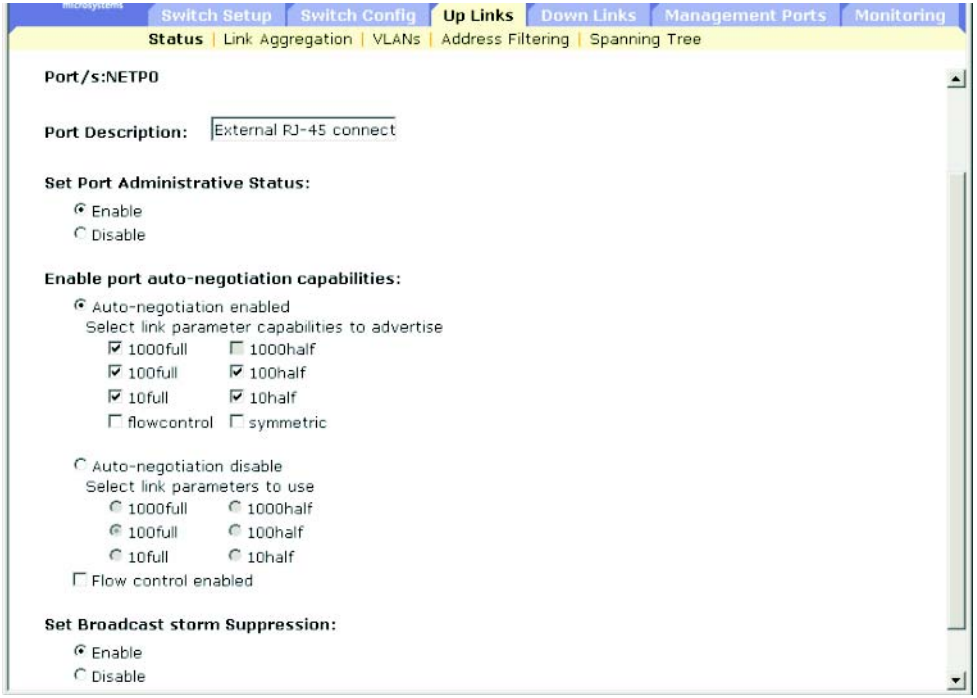
- **Speed/Duplex**[2] **:** Lorsque l'auto-négociation est désactivée, vous pouvez configurer manuellement la vitesse et le mode duplex du port.

Remarque - Lorsque l'auto-négociation est désactivée, vous pouvez uniquement définir les ports à liaison ascendante à 10 Mbps ou 100 Mbps. Pour forcer un port à fonctionner à 1 Gbps en duplex, activez l'auto-négociation et définissez les capacités du port à « 1000full » uniquement.

- **Flow Control**[2] **:** Lorsque l'auto-négociation est désactivée, vous devez activer ou désactiver le contrôle de flux. (Evitez d'utiliser le contrôle de flux sur un port connecté à un concentrateur, à moins qu'il soit effectivement requis pour résoudre un problème, sans quoi les signaux de brouillage de la contre-pression peuvent amoindrir les performances globales du segment attaché au concentrateur).
- **Broadcast storm suppression :** Active la suppression des orages de diffusion pour le(s) port(s) sélectionné(s). Pour plus d'informations sur le contrôle des orages de diffusion ou sur la définition du seuil de diffusion, reportez-vous à « Contrôle des orages de diffusion (Global Setting) » à la page 3-55.

1. L'auto-négociation ne peut pas être désactivée sur les ports à liaison descendante. Ces ports sont fixés à 1000 Mbps, duplex.
2. L'auto-négocation doit être désactivée sur les ports à liaison ascendante avant que vous puissiez configurer l'interface ou la forcer à utiliser une vitesse, un mode duplex ou une option de contrôle de flux spécifiques.

Web : Ouvrez l'écran Up Links / Down Links=>Status. Cochez les cases des interfaces à configurer, puis cliquez sur Configure. Modifiez les paramètres d'interface requis, et cliquez sur Save.



ILC : Sélectionnez l'interface, puis entrez les paramètres requis.

```
Console#Console(config)#interface ethernet NETP1 4-74
Console(config-if)#description RD SW#17                    4-75
Console(config-if)#shutdown                                4-80
.
.
.
Console(config-if)#no shutdown
Console(config-if)#negotiation
Console(config-if)#capabilities 1000full                   4-78
Console(config-if)#capabilities 1000full 4-78
Console(config-if)#capabilities flowcontrol
.
.
.
Console(config-if)#no negotiation 4-77
Console(config-if)#speed-duplex 100half 4-75
Console(config-if)#flowcontrol 4-79
Console(config-if)#
```

SNMP : Variables MIB équivalentes.

Nom de zone	Variable MIB	Accès	Plage de valeurs	Valeur par défaut
Port Name	sun... portMgt. portTable.portEntry. portName	Lecture/ Ecriture	Chaîne d'affichage (Taille (0-64))	Page 4-84
Administrative Status	MIB-II. interfaces. ifTable.ifEntry. ifAdminStatus	Lecture/ Ecriture	up (1), down (2), testing (3)	up
Port Auto-negotiation	sun... portMgt. portTable.portEntry. portAutonegotiation	Lecture/ Ecriture	enabled (1), disabled (2)	enabled
Port Capabilities	sun... portMgt. portTable.portEntry. portCapabilities	Lecture/ Ecriture	Bits{ portCap10half (0), portCap10full (1), portCap100half (2), portCap100full (3), portCap1000half (4), portCap1000full (5), reserved6-13 (6-13), portCapSym (14), portCapFlowCtrl (15)}	
Port Speed Duplex Configuration	sun... portMgt. portTable.portEntry. portSpeedDpxCfg	Lecture/ Ecriture	reserved(1), halfDuplex10(2), halfDuplex10(3), halfDuplex100(4), fullDuplex100(5), halfDuplex1000(6), fullDuplex1000(7)	
Port Flow Control Configuration	sun... portMgt. portTable.portEntry. portFlowCtrlCfg	Lecture/ Ecriture	enabled (1), backPressure(2), dot3xFlowControl(4),	

3.4.3 Configuration du regroupement de ports

Vous pouvez rassembler plusieurs liaisons établies entre des périphériques afin qu'elles fonctionnent comme une liaison unique virtuelle. Un groupe de ports permet une augmentation considérable de la bande passante pour les segments du réseau où il existe des goulots d'étranglement et propose une liaison tolérant les défauts entre deux périphériques. Vous pouvez créer jusqu'à six groupes en une seule fois.

Le commutateur prend en charge le regroupement statique et le protocole dynamique LACP (Link Aggregation Control Protocol). Les ports configurés en LACP négocient automatiquement une liaison groupée avec les ports configurés en LACP d'un autre périphérique. Vous pouvez configurer autant de ports à liaison ascendante que vous le souhaitez sur le commutateur à l'aide du LACP, pour autant que ces ports ne fassent pas déjà partie d'un groupe statique. Si les ports d'un autre périphérique sont également configurés à l'aide du LACP, le commutateur et l'autre périphérique négocient une liaison groupées entre eux. Si un groupe LACP comporte plus de quatre ports, tous les autres ports passent en mode veille. Si une liaison du groupe est défaillante, l'un des ports en veille est automatiquement activé pour la remplacer.

Utilisation de la commande

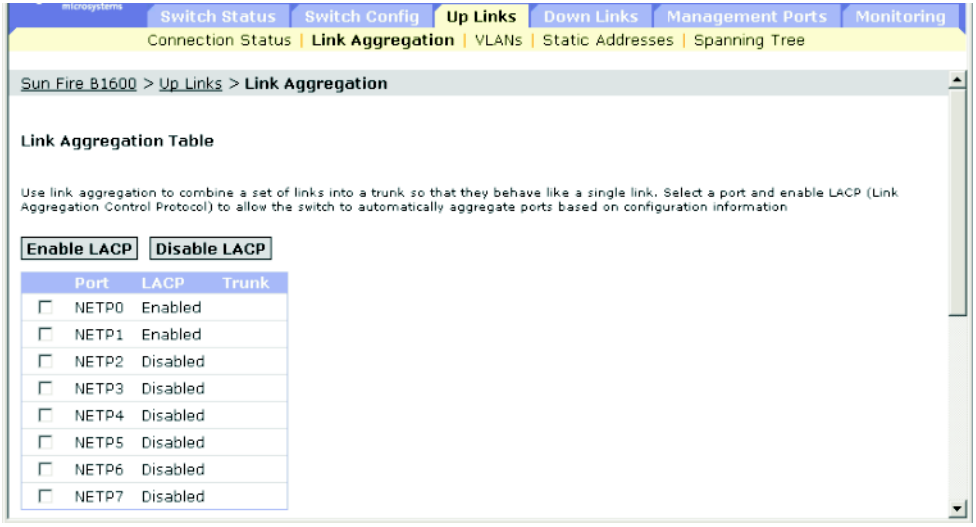
Outre la répartition de la charge entre les ports d'un groupe, les ports supplémentaires assurent la redondance en reprenant la charge si un port du groupe s'avère défaillant. Toutefois, avant d'établir des connexions physiques entre les périphériques, utilisez l'interface Web ou l'ILC pour spécifier le groupe sur les périphériques situés aux deux extrémités de la connexion. Lorsque vous utilisez un groupe de ports, ne perdez pas les points suivants de vue :

- Terminez la configuration des groupes de ports avant de connecter les câbles réseau correspondants entre les commutateurs pour éviter de créer une boucle.
- Vous pouvez créer jusqu'à six groupes sur le commutateur, chacun pouvant contenir jusqu'à quatre ports.
- Les ports situés aux deux extrémités d'une connexion doivent être configurés comme ports du groupe.
- Les ports situés aux deux extrémités d'un groupe doivent être configurés d'une manière identique, en ce compris le mode de communication (vitesse, mode duplex et contrôle de flux), les affectations au VLAN et les paramètres CdS.
- Si le commutateur cible a également activé le LACP sur les ports connectés, le groupe est activé automatiquement.
- Un groupe formé avec un autre commutateur à l'aide du LACP reçoit automatiquement le premier identificateur de groupe disponible.
- Si plus de quatre ports attachés au même commutateur cible ont un LACP actif, les ports supplémentaires passent en mode veille et ne sont activés que si l'une des liaisons actives tombe en panne.
- Tous les ports d'un groupe doivent être traités comme un ensemble lorsqu'ils sont déplacés depuis/vers un VLAN, lui sont ajoutés ou en sont supprimés.
- Les paramètres STP, VLAN et IGMP ne peuvent être définis que pour l'ensemble du groupe.

3.4.3.1 Configuration dynamique d'un groupe à l'aide du protocole LACP

Web : Cliquez sur Up Links / Down Links=>Link Aggregation. Localisez le port requis dans la table Link Aggregation, et cliquez sur le bouton Enable LACP ou Disable LACP.

Remarque - Les boutons d'action sont immédiatement activés. Pour éviter de créer une boucle réseau, veillez à activer le LACP avant de connecter les ports et de déconnecter les ports avant de désactiver le LACP. Reportez-vous à l'utilisation de la commande à la page 4-88.



ILC : L'exemple suivant active le LACP pour les ports NETP0 et NETP1. Il vous suffit de connecter ces ports aux deux ports de groupes avec le LACP actif sur un autre commutateur pour former un groupe.

```
Console(config)#interface ethernet NETP0 4-74
Console(config-if)#lacp                                    4-147
Console(config-if)#exit
Console(config)#interface ethernet NETP1
Console(config-if)#lacp
Console(config-if)#end
Console#show interfaces status port-channel 1 4-83
Information of Trunk 1
Basic information:
  Port type: 1000T
  Mac address: 00-00-E8-66-66-83
 Configuration:
  Name:
  Port admin: Up
  Speed-duplex: Auto
  Capabilities: 10half, 10full, 100half, 100full, 1000full,
  Flow control status: Disabled
```

```
 Current status:
  Created by: Lacp
  Link status: Up
  Port operation status: Up
  Operation speed-duplex: 1000full
  Flow control type: None
  Member Ports: NETP0, NETP1,
Console#
```

SNMP : Variables MIB équivalentes.

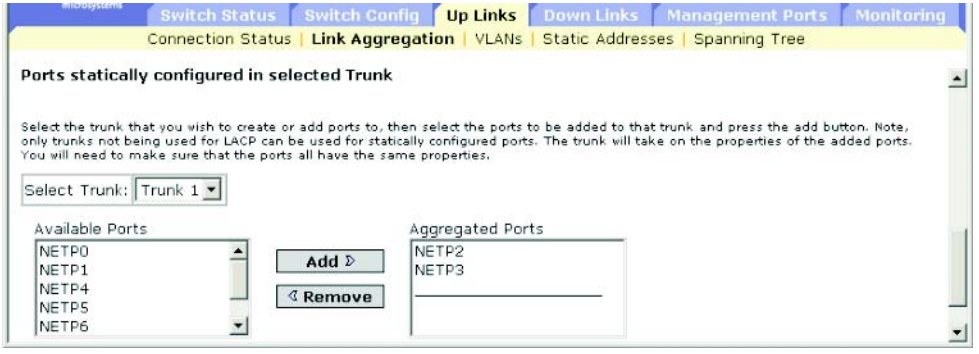
Nom de zone	Variable MIB	Accès	Plage de valeurs	Valeur par défaut
Trunk Maximum ID	sun... trunkMgt. trunkMaxId	Lecture seule	Nombre entier	6
Trunk Valid Number	sun... trunkMgt. trunkValidNumber	Lecture seule	Nombre entier (1-6)	
Trunk Index	sun... trunkMgt. trunkTable.trunkEntry. trunkIndex	Index	Nombre entier	
Trunk Ports	sun... trunkMgt. trunkTable.trunkEntry. trunkPorts	Lecture/ Création	Chaîne d'octets (Liste des ports)	
Trunk Creation	sun... trunkMgt. trunkTable.trunkEntry. trunkCreation	Lecture seule	static (1), lacp (2)	
Trunk Status	sun... trunkMgt. trunkTable.trunkEntry. trunkStatus	Lecture/ Création	valid (1), invalid (2)	
LACP Port Status	sun... lacpMgt. lacpPortTable. lacpPortEntry. lacpPortStatus	Lecture/ Ecriture	enabled (1) disabled (2)	

Pour obtenir une description des autres variables de l'ILC, reportez-vous à « Affichage de l'état de la connexion » à la page 3-80

3.4.3.2 Configuration statique d'un groupe

Web : Cliquez sur Up Links / Down Links=>Link Aggregation. Sélectionnez l'index du groupe dans la liste déroulante, choisissez le port requis, puis cliquez sur Add ou Remove.

Remarque - Les boutons d'action sont immédiatement activés. Pour éviter de créer une boucle réseau, veillez à ajouter un groupe statique via l'interface de configuration avant de connecter les ports et à déconnecter les ports avant de supprimer un groupe statique via l'interface de configuration. Reportez-vous à l'utilisation de la commande à la page 4-88.



ILC : L'exemple suivant crée un groupe 2 avec les ports NETP2 et NETP3. Il vous suffit de connecter ces ports à deux ports statiques appartenant à un groupe sur un autre commutateur pour former un groupe.

```
Console(config)#interface port-channel 24-74
Console(config-if)#exit
Console(config)#interface ethernet NETP24-74
Console(config-if)#channel-group 24-146
Console(config-if)#exit
Console(config)#interface ethernet NETP3
Console(config-if)#channel-group 2
Console(config-if)#end
Console#show interfaces status port-channel 24-83
Information of Trunk 2
 Basic information:
  Port type: 1 000t
  Mac address: 00-00-E8-66-66-83
 Configuration:
Port admin status: Up
  Speed-duplex: Auto
  Capabilities: 10half, 10full, 100half, 100full, 1000full,
  Flow control status: Disabled
```

```
 Current status:
  Created by: User
  Link status: Up
  Port operation status: Up
  Operation speed-duplex: 1000full
  Flow control type: None
  Member Ports: NETP2, NETP3,
Console#
```

SNMP : Variables MIB équivalentes.

Nom de zone	Variable MIB	Accès	Plage de valeurs	Valeur par défaut
Trunk Maximum ID	sun... trunkMgt.trunkMaxId	Lecture seule	Nombre entier	6
Trunk Valid Number	sun... trunkMgt. trunkValidNumber	Lecture seule	Nombre entier (1-6)	
Trunk Index	sun... trunkMgt.trunkTable. trunkEntry.trunkIndex	Index	Nombre entier	
Trunk Ports	sun... trunkMgt.trunkTable. trunkEntry.trunkPorts	Lecture/ Création	Chaîne d'octets (Liste des ports)	
Trunk Creation	sun... trunkMgt. trunkTable.trunkEntry. trunkCreation	Lecture seule	static (1), lacp (2)	
Trunk Status	sun... trunkMgt.trunkTable. trunkEntry.trunkStatus	Lecture/ Création	valid (1), invalid (2)	

Pour obtenir une description des autres variables de l'ILC, reportez-vous à « Affichage de l'état de la connexion » à la page 3-80

3.4.4 Configuration du comportement des VLAN pour les interfaces

Vous pouvez configurer le comportement des VLAN pour les interfaces spécifiques, y compris l'identificateur du VLAN par défaut (PVID), les types de trames acceptées, le filtrage à l'entrée, l'état GVRP et les horloges GARP.

Utilisation de la commande

- **GVRP** : Le protocole GVRP (GARP VLAN Registration Protocol) définit une méthode permettant aux commutateurs d'échanger des informations sur le VLAN afin d'enregistrer automatiquement les membres des VLAN sur les interfaces du réseau.
- **GARP** : Le protocole GARP (Group Address Registration Protocol) est utilisé par le GVRP pour enregistrer ou désenregistrer les attributs du client pour les services clients dans un LAN muni de ponts. Les valeurs par défaut des horloges GARP sont indépendantes de la méthode d'accès aux supports ou des taux de données. Ces valeurs ne doivent pas être modifiées à moins que vous ne rencontriez des difficultés avec l'enregistrement/désenregistrement GVRP.

Attributs des commandes

- **Port** : Port ou groupe (liaisons ascendantes : NETP0-7, liaisons descendantes : SNP0-15, gestion : NETMGT).
- **Default VLAN for Port (PVID)** : identificateur du VLAN affecté aux trames non marquées reçues sur une interface. (Par défaut : Liaisons ascendantes/ descendantes : 1 ; NETMGT : 2)

Remarque : Si une interface n'est pas membre du VLAN 1 et si vous affectez son PVID au VLAN 1, l'interface est ajoutée automatiquement au VLAN 1 sous la forme d'un membre non marqué. Pour tous les autres VLAN, il convient de configurer d'abord une interface sous la forme d'un membre non marqué avant de pouvoir affecter son PVID à ce groupe.

- **Acceptable Frame Types** : Définit l'interface afin que celle-ci accepte tous les types de trames, y compris les trames marquées ou non marquées, ou seulement les trames marquées. Lorsque cette option est définie de sorte à recevoir tous les types de trames, les trames non-marquées reçues sont affectées au VLAN par défaut. (Options : all, tagged ; Par défaut : all)
- **Switch Port Mode** : Indique le mode d'appartenance au VLAN pour un port. (Par défaut : groupe)
  - **Trunk** : Spécifie un port comme point final pour un groupe de VLAN. Un groupe représente une liaison directe entre deux commutateurs permettant au port de transmettre des trames marquées qui identifient le VLAN source.
  - **Hybrid** : Spécifie une interface VLAN hybride. Le port peut transmettre des trames marquées ou non marquées.

Remarque : Si le mode du port du commutateur a la valeur **Trunk**, les trames appartenant au VLAN par défaut du port (à savoir le VLAN associé au PVID) sont envoyées sans marque, mais toutes les autres trames sont marquées par l'identificateur du VLAN affecté.

- **Ingress Filtering** : Si le filtrage à l'entrée est activé, les trames entrantes pour les VLAN qui ne comptent pas le port d'entrée parmi leurs membres seront ignorées au niveau de ce port. (Par défaut : désactivé)

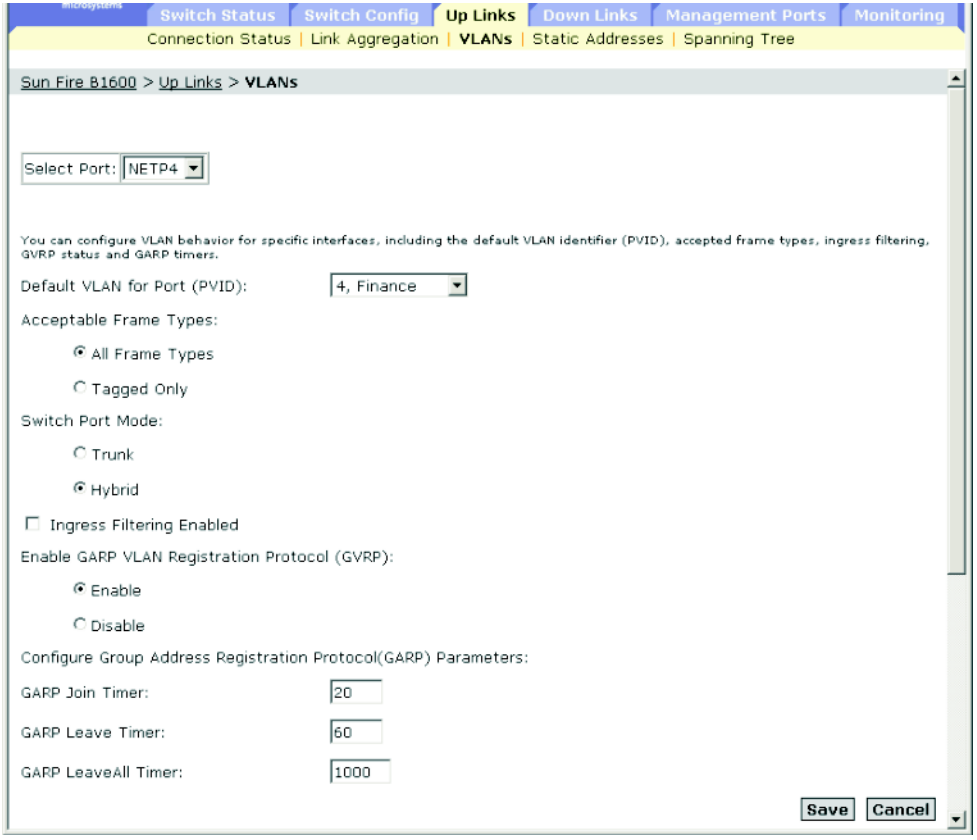
Remarques :

- Le filtrage à l'entrée n'affecte que les trames marquées.
- Si le filtrage à l'entrée est désactivé, l'interface accepte les trames marquées VLAN si la marque correspond à un VLAN connu du commutateur (sauf les VLAN explicitement interdits sur ce port).
- Dans le cas contraire, l'interface ignore les trames entrantes marquées pour des VLAN qui ne comptent pas ce port d'entrée parmi leurs membres.
- Le filtrage à l'entrée n'affecte pas les trames BPDU indépendantes du VLAN, telles que GVRP ou STP. Toutefois, il touche les trames BPDU dépendantes du VLAN, telles que GMRP.

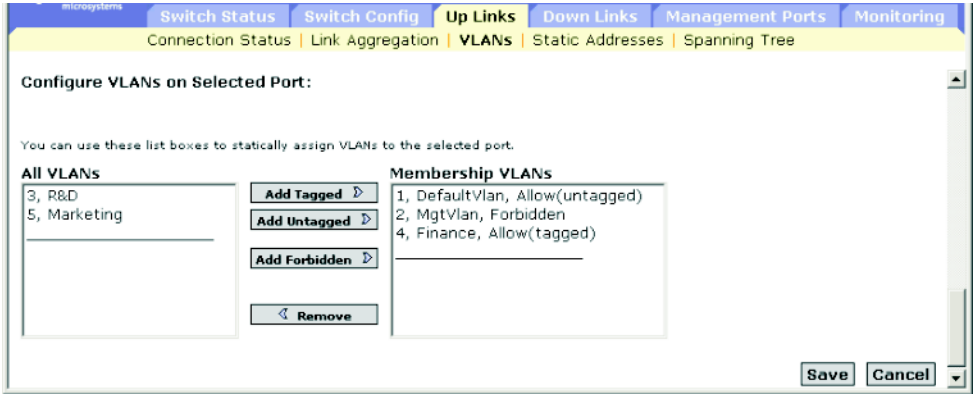
- **GVRP :** Active/désactive le GVRP pour l'interface. Le GVRP doit être activé globalement pour le commutateur avant que ce paramètre puisse prendre effet (page 4-39.) Lorsque cette option est désactivée, tous les paquets GVRP reçus sur ce port sont ignorés et aucun enregistrement GVRP n'est propagé depuis d'autres ports. (Par défaut : désactivé)
- **GARP Join Timer** : Intervalle entre les demandes de transmission/requêtes visant à participer à un groupe de VLAN.
  (Plage : 20-1000 centisecondes ; par défaut : 20 centisecondes)
- **GARP Leave Timer** : Délai d'attente d'un port avant que celui-ci quitte un groupe de VLAN. Ce délai doit être au moins le double du délai GARP Join Timer. Ceci garantit qu'après l'émission d'un message Leave ou LeaveAll, les candidats puissent adhérer au groupe avant que le port ne quitte celui-ci effectivement.
  (Plage : 60-3000 centisecondes ; par défaut : 60 centisecondes)
- **GARP LeaveAll Timer** : Intervalle entre l'envoi d'un message LeaveAll aux participants d'un groupe de VLAN et le départ effectif du port de ce groupe. L'intervalle doit être considérablement supérieur au Leave Time afin de réduire la quantité de trafic générée par les noeuds adhérant au groupe.
  (Plage : 500-18000 centisecondes ; par défaut : 1000 centisecondes)
- **VLANs on Selected Port :** Affectation statique du port au VLAN spécifié.
- **Membership Type** : Définit l'appartenance statique du port à un VLAN.

- **Tagged** : L'interface est membre du VLAN. Tous les paquets transmis par le port sur ce VLAN sont marqués. En d'autres termes, ils sont porteurs d'une marque et contiennent donc des informations sur le VLAN ou la CdS.
- **Untagged** : L'interface est membre du VLAN. Aucun paquet transmis par le port sur ce VLAN n'est marqué. En d'autres termes, ils ne sont pas porteurs de marque et ne contiennent donc pas d'informations sur le VLAN ou la CdS.
- **Forbidden** : Il est interdit à l'interface d'adhérer au VLAN automatiquement via le GVRP. Reportez-vous à « Enregistrement automatique du VLAN » à la page 4-35.
- **Remove** : Supprime l'interface sélectionnée de ce VLAN.

Web : Ouvrez Up Links / Down Links / Management Port=>VLANs. Renseignez les paramètres requis pour chaque interface, puis cliquez sur Save.



Faites défiler le tableau des membres du VLAN vers le bas, et configurez les VLAN requis pour l'interface sélectionnée.



ILC : Cet exemple définit le port NETP4 afin que celui-ci n'accepte que les trames marquées, affecte PVID 4 comme identificateur naturel du VLAN, active le GVRP, définit les horloges GARP, puis définisse un mode de port de commutateur hybride.

```
Console(config)#interface ethernet NETP4 4-74
Console(config-if)#switchport acceptable-frame-types tagged 4-109
Console(config-if)#no switchport ingress-filtering 4-110
Console(config-if)#switchport allowed vlan add 4 tagged      4-112
Console(config-if)#switchport native vlan 4 4-111
Console(config-if)#switchport gvrp 4-115
Console(config-if)#garp timer join 10 4-117
Console(config-if)#garp timer leave 90 4-117
Console(config-if)#garp timer leaveall 2000 4-117
Console(config-if)#switchport mode hybrid 4-108
Console(config-if)#switchport forbidden vlan add 3           4-113
Console(config-if)#
```

SNMP : Variables MIB équivalentes.

Nom de zone	Variable MIB	Accès	Plage de valeurs	Valeur par défaut
Port PVID	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qPortVlanTable. dot1qPortVlanEntry. dot1qPvid	Lecture/ Ecriture	Nombre entier (1-4094)	1
Port Acceptable Frame Type	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qPortVlanTable. dot1qPortVlanEntry. dot1qPortAcceptable-FrameTypes	Lecture/ Ecriture	admitAll (1), admitOnlyVlan-Tagged (2)	admitAll
Port Mode	sun... vlanMgt. vlanPortTable. vlanPortEntry. vlanPortMode	Lecture/ Ecriture	hybrid (1), dot1qTrunk (2)	hybrid
Port Ingress Filtering	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qPortVlanTable. dot1qPortVlanEntry. dot1qPortIngressFiltering	Lecture/ Ecriture	true (1), false (2)	false
Port GVRP Status	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qPortVlanTable. dot1qPortVlanEntry. dot1qPortGVRPStatus	Lecture/ Ecriture	enabled (1), disabled (2)	disabled

Nom de zone	Variable MIB	Accès	Plage de valeurs	Valeur par défaut
GARP Join Time	MIB-II. dot1dBridge. pBridgeMIB. pBridgeMIBObjects. dot1dGarp. dot1dPortGarpTable. dot1dPortGarpEntry. dot1dPortGarpJoinTime	Lecture/ Ecriture	Nombre entier (20-1000) centisecondes	20 centisecondes
GARP Leave Time	MIB-II. dot1dBridge. pBridgeMIB. pBridgeMIBObjects. dot1dGarp. dot1dPortGarpTable. dot1dPortGarpEntry. dot1dPortGarpLeaveTime	Lecture/ Ecriture	Nombre entier (60-3000) centisecondes	60 centisecondes
GARP Leave All Time	MIB-II. dot1dBridge. pBridgeMIB. pBridgeMIBObjects. dot1dGarp. dot1dPortGarpTable. dot1dPortGarpEntry. dot1dPortGarp- LeaveAllTime	Lecture/ Ecriture	Nombre entier (500-18000) centisecondes	1000 centisecondes
VLAN Static Name	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanStaticTable. dot1qVlanStaticEntry. dot1qVlanStaticName	Lecture/ Création	Chaîne d'octets (Taille (0-32))-	
VLAN Static Row Status	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanStaticTable. dot1qVlanStaticEntry. dot1qVlanStatic.	Lecture/ Création	enable(1), disable(2)	

Nom de zone	Variable MIB	Accès	Plage de valeurs	Valeur par défaut
Tagged Ports, Untagged Ports (Allowed VLAN)	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanTable. dot1qVlanEntry. dot1qVlanStatic-UntaggedPorts	Lecture/ Création	Chaîne d'octets (Liste des ports)	
VLAN Forbidden Ports	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qPortVlanTable. dot1qPortVlanEntry. dot1qVlanForbidden-EgressPorts	Lecture/ Création	Chaîne d'octets (Liste des ports)	

3.4.5 Configuration d'adresses statiques

Vous pouvez utiliser le filtrage des adresses pour définir des adresses statiques liées à un port et à un VLAN spécifiques, ou pour activer la sécurité d'un port visant à limiter le trafic entrant aux entrées figurant actuellement dans la table d'adressage (adresses dynamiques ou statiques).

Utilisation de la commande

- **Setting Static Addresses** : Une adresse statique peut être affectée à une interface spécifique sur ce commutateur. Quand une adresse statique actuellement liée à une interface est visible sur une autre interface, la nouvelle interface qui la détecte n'accepte et ne transmet aucune donnée provenant de ou destinée à cette adresse et n'inclut pas l'adresse dans sa table d'adressage.
- **Configuring Port Security** : Si vous activez la sécurité du port, le commutateur cesse l'apprentissage dynamique de nouvelles adresses sur le port spécifié. Seul le trafic entrant avec des adresses source déjà stockées dans la table d'adressage dynamique est accepté. Pour utiliser la sécurité du port, autorisez d'abord le commutateur à apprendre dynamiquement <l'adresse MAC source, la >paire VLAN pour les trames reçues sur une interface pour une période préparatoire initiale, puis activez la sécurité du port pour cesser l'apprentissage des adresses. Veillez à activer la fonction d'apprentissage suffisamment longtemps pour vous assurer que tous les membres du VLAN valables ont été enregistrés sur l'interface sélectionnée.

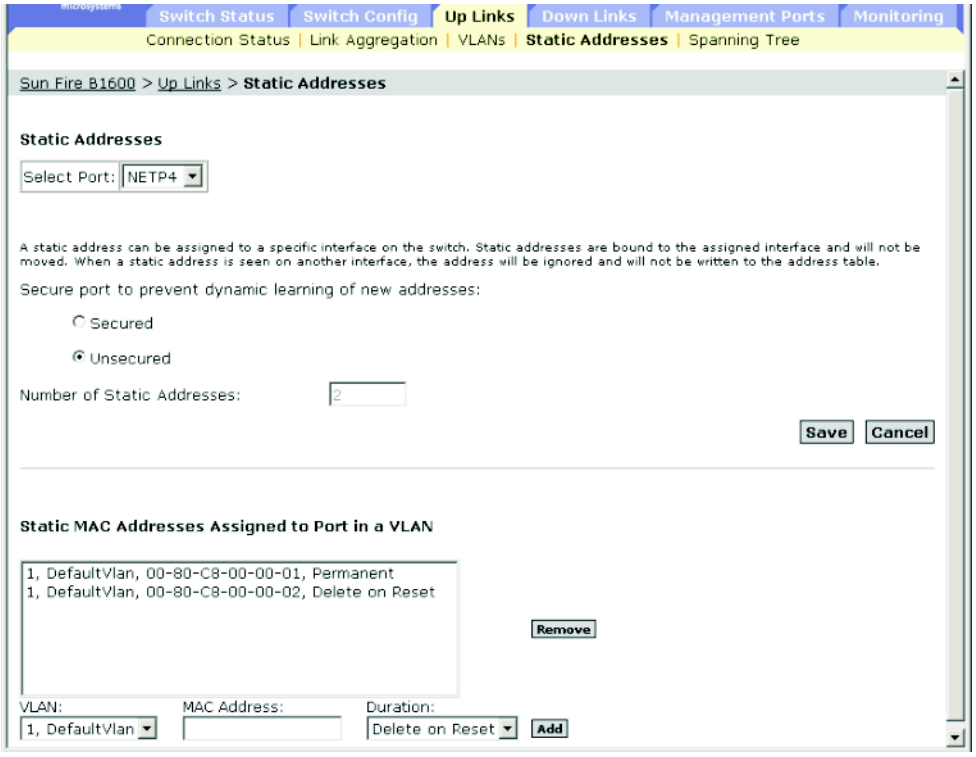
  Pour ajouter de nouveaux membres au VLAN ultérieurement, vous pouvez ajouter des adresses statiques manuellement ou désactiver la sécurité du port afin de réactiver la fonction d'apprentissage suffisamment longtemps pour que les nouveaux membres VLAN puissent être enregistrés. Si vous le souhaitez, vous pouvez alors désactiver l'apprentissage une nouvelle fois, à des fins de sécurité.

Attributs des commandes

- **Port** : Interface (port ou groupe).
  (Ports à liaison ascendante : NETP0-7, ports à liaison descendante : SNP0-15)
- **Secure Port** : Active ou désactive la sécurité du port. (Par défaut : désactivée)
  Un port sécurisé présente les restrictions suivantes :
  - utilisation de la surveillance du port impossible ;
  - fonctionnement en tant qu'interface multi-VLAN impossible ;
  - connexion à un périphérique d'interconnexion réseau impossible ;
  - fonctionnement en tant que port de groupe impossible.
- **Number of Static Addresses*** : Nombre d'adresses configurées manuellement.
- **VLAN** : Identificateur et nom du VLAN (1-4094) configuré.
- **MAC Address** : Adresse MAC associée à cette interface.
- **Duration** : L'adresse peut être définie au type suivant :
  - **Permanent** : L'affectation est permanente et restaurée après la réinitialisation du commutateur.
  - **Delete on Reset** : L'affectation dure jusqu'à ce que le commutateur soit réinitialisé.

* Web uniquement

Web : Ouvrez Up Links / Down Links=>Address Filtering. Spécifiez l'interface. Cochez la case Secure Port pour activer la sécurité du port. Ensuite, entrez le VLAN, l'adresse MAC et la durée, puis cliquez sur Add.



ILC : Cet exemple ajoute les mêmes éléments à la table des adresses statiques.

```
Console(config)#interface ethernet NETP4
Console(config-if)#port security4-91
Console(config-if)exit
Console(config)#mac-address-table static 00-80-c8-00-00-01
  interface ethernet NETP4 vlan 1 permanent4-87
Console(config)#mac-address-table static 00-80-c8-00-00-02
  interface ethernet NETP4 vlan 1 delete-on-reset
Console(config)#exit
Console#show mac-address-table ethernet NETP44-88
 Interface   Mac Address       Vlan Type
 ----------- ----------------- ---- -----------------
       NETP4 00-80-C8-00-00-01    1 Permanent
       NETP4 00-80-C8-00-00-02    1 Delete-on-reset
Console#
```

SNMP : Variables MIB équivalentes.

Nom de zone	Variable MIB	Accès	Plage de valeurs	Valeur par défaut
Static Receive Port	MIB-II. dot1dBridge. dot1dStatic. dot1dStaticTable. dot1dStaticEntry. dot1dStaticReceivePort	Lecture/ Ecriture	Nombre entier	
Port Security Status	sun... securityMgt. portSecurityMgt portSecPortTable. portSecPortEntry. portSecPortStatus	Lecture/ Ecriture	enabled (1), disabled (2)	disabled
Number of Static Addresses	*Non défini*			
VLAN Index	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanStaticTable. dot1qVlanStaticEntry. dot1qVlanIndex	Index	Nombre entier	
Static Address	MIB-II. dot1dBridge. dot1dStatic. dot1dStaticTable. dot1dStaticEntry. dot1dStaticAddress	Lecture/ Ecriture	Adresse MAC	
Static Status	MIB-II. dot1dBridge. dot1dStatic. dot1dStaticTable. dot1dStaticEntry. dot1dStaticStatus	Lecture/ Ecriture	other(1), invalid (2) permanent(3), deleteOnReset(4), deleteOnTimeout(5)	permanent

3.4.6 Gestion des interfaces pour l'algorithme Spanning Tree

Vous pouvez configurer les attributs RSTP pour des interfaces spécifiques, et notamment la priorité du port, la distance à parcourir et le port de périphérie. Il est possible d'utiliser une priorité ou distance à parcourir différente pour les ports du même type de support pour indiquer le chemin préféré, le type de liaison pour indiquer une connexion point-par-point ou une connexion de support partagé, et un port de périphérie pour indiquer si le périphérique attaché peut prendre en charge la transmission rapide.

3.4.6.1 Affichage des paramètres de l'interface courante pour le STA

Attributs des commandes

- **Port** : Ports uniquement ; à savoir aucun groupe ou port membre du groupe. (Ports à liaison ascendante : NETP0-7, ports à liaison descendante : SNP0-15)
- **STA Status :** Affiche l'état courant de ce port dans le Spanning Tree :
  - **Discarding** : Le port reçoit les messages de configuration STA, mais ne peut transmettre des paquets.
  - **Learning** : Le port a transmis des messages de configuration pour un intervalle défini par le paramètre Forward Delay sans recevoir d'informations contradictoires. La table d'adressage des ports est vidée, et le port commence à apprendre les adresses.
  - **Forwarding** : Le port transmet des paquets, et continue à apprendre les adresses.
- **Priority** : Définit la priorité utilisée pour ce port dans l'algorithme Spanning Tree. Si la distance à parcourir pour tous les ports sur un commutateur est la même, le port avec la priorité la plus élevée (à savoir la valeur la plus basse) sera configuré comme liaison active dans le Spanning Tree. Cette option rend le port avec la priorité la plus élevée moins susceptible d'être bloqué si l'algorithme Spanning Tree détecte des boucles réseau. Si plus d'un port reçoit la priorité la plus élevée, le port activé est celui avec l'identificateur numérique le plus bas.
- **Path Cost** : Ce paramètre est utilisé par le STA pour déterminer le meilleur chemin entre les périphériques. C'est pourquoi les valeurs inférieures doivent être affectées aux ports attachés aux supports les plus rapides, et les valeurs supérieures aux ports avec les supports les plus lents. (Le coût du chemin est prioritaire sur la priorité du port).
- **Designated Cost** : Coût requis pour le déplacement d'un paquet entre le port et la racine dans la configuration courante du Spanning Tree. Plus le support est lent, plus le coût est élevé.
- **Designated Bridge** : Priorité et l'adresse MAC du périphérique par le biais duquel ce port doit communiquer pour atteindre la racine du Spanning Tree.
- **Designated Port** : La priorité et le numéro du port sur le périphérique-pont désigné par le biais duquel ce commutateur doit communiquer avec la racine du Spanning Tree.

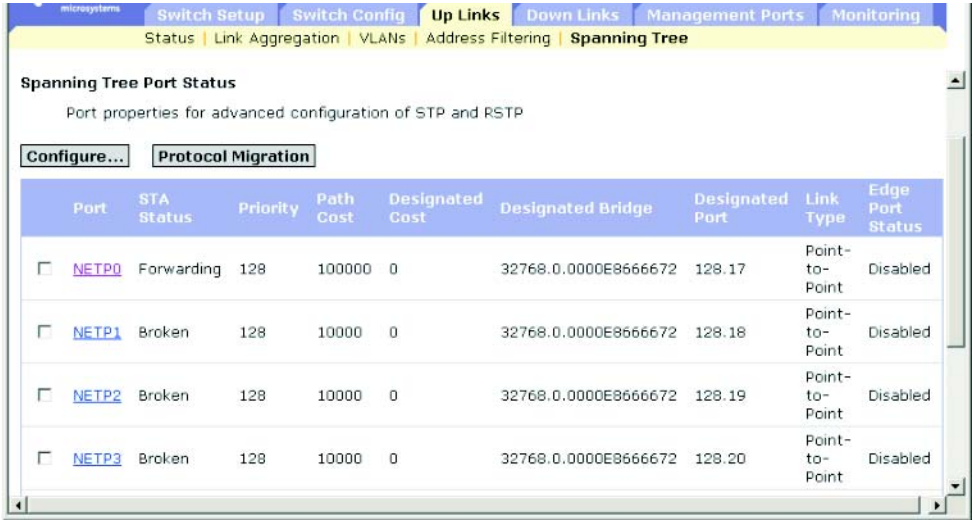
- **Link Type** (Admin Link type*) : Type de lien attaché à cette interface.
  - Point-par-point : Connexion à un seul autre pont.
  - Partagé : Connexion à deux ou plusieurs ponts.
  - Auto : Le commutateur détermine automatiquement si l'interface est attachée à un lien point-par-point ou à un support partagé.
- **Edge Port** (Port de périphérie Admin*) : Vous pouvez activer cette option si une interface est attachée à un segment LAN qui se trouve à la fin d'un LAN ponté ou sur un noeud terminal. Etant donné que les noeuds finaux **ne peuvent pas** provoquer de boucles de transmission, ils peuvent passer directement à l'état de transmission du Spanning Tree. Spécifier les ports marginaux permet une convergence plus rapide pour les périphériques tels que les stations de travail ou les serveurs, conserve la base de données de transmission courante pour réduire la quantité d'envoi de cadres requise pour reconstruire les tables d'adresses pendant les événements de reconfiguration, ne pousse pas le Spanning Tree à initier la reconfiguration lorsque l'interface change d'état et surmonte également d'autres problèmes de temporisation liés au STA. Toutefois, rappelez-vous que le port de périphérie ne doit être activé que pour les ports connectés à un périphérique de noeud final.

* L'ILC affiche ce terme.

Les paramètres supplémentaires suivants ne sont affichés que pour l'ICL :

- **Admin Status :** Indique si le STA a été activé sur cette interface.
- **Role** : Les rôles sont affectés selon que le port appartient à la topologie active reliant le pont au pont racine (en d'autres termes, le port **racine**), reliant un LAN au pont racine (en d'autres termes, le **port désigné**) par le biais du pont ; ou s'il s'agit d'un port **alternatif** ou **de sauvegarde** permettant une connectivité si d'autres ponts, ports-ponts ou LAN sont défaillants ou disparaissent. Le rôle est désactivé (en d'autres termes, port **désactivé**) si un port ne joue aucun rôle dans le Spanning Tree.
- **Designated root** : Priorité et adresse MAC du périphérique Spanning Tree que ce commutateur a accepté comme périphérique racine.
- **Forward transitions** : Nombre de transitions de ce port entre l'état Apprendre et l'état Transmettre.
- **Oper edge port** : Ce paramètre est initialisé à la définition du port Admin Edge Port (à savoir vrai ou faux), mais reçoit la valeur « false » si un BPDU est réceptionné.
- **Oper Link type** : Etat point-par-point opérationnel du segment LAN attaché à cette interface. Ce paramètre est déterminé par configuration manuelle ou par auto-détection, tel que décrit pour Admin Link Type.

Web : Cliquez sur Up Links / Down Links=>Spanning Tree=>Spanning Tree Protocol.



ILC : Cet exemple affiche les attributs STA pour le port NETP4.

```
Console#show spanning-tree ethernet NETP4-103
SNP0 information
---------------------------------------------------------------
 Admin status          : enable
 Role                  : designate
 State                 : forwarding
 Path cost             : 10000
 Priority              : 128
 Designated cost       : 10000
 Designated port       : 128.1
 Designated root       : 32768.00209C23C267
 Designated bridge     : 32768.0000E8666672
 Forward transitions   : 0
 Admin edge port       : disable
 Oper edge port        : disable
 Admin Link type       : point-to-point
 Oper Link type        : point-to-point
Console#
```

SNMP : Variables MIB équivalentes.

Nom de zone	Variable MIB	Accès	Plage de valeurs	Valeur par défaut
Port	sun...xstMgt. mstInstancePortTable. mstInstancePortEntry	Index	Nombre entier (1-25)	
STA Port State	sun...xstMgt. mstInstancePortTable. mstInstancePortEntry. mstInstancePortState	Lecture seule	discarding (1), learning (2), forwarding (3)	
STA Port Priority	sun...xstMgt. mstInstancePortTable. mstInstancePortEntry. mstInstancePortPriority	Lecture/ Ecriture	Nombre entier (0-240)	128
STA Port Path Cost	sun...xstMgt. mstInstancePortTable. mstInstancePortEntry. mstInstancePortPathCost	Lecture/ Ecriture	Nombre entier (long : 1-200 000 000 ; court : 1-65 535)	page 4-107
STA Port Designated Cost	sun...xstMgt. mstInstancePortTable. mstInstancePortEntry. mstInstancePort-DesignatedCost	Lecture seule	Nombre entier	
STA Port Designated Bridge	sun...xstMgt. mstInstancePortTable. mstInstancePortEntry. mstInstancePort-DesignatedBridge	Lecture seule	Chaîne d'octets	
STA Port Designated Port	sun...xstMgt. mstInstancePortTable. mstInstancePortEntry. mstInstancePort-DesignatedPort	Lecture seule	Chaîne d'octets	
STA Port Admin Point to Point	sun...staMgt. staPortTable. staPortEntry. staPortAdminPointTo-Point	Lecture/ Ecriture	forceTrue(0) forceFalse (1) auto (2),	auto
STA Port Admin Edge Port	sun...staMgt. staPortTable. staPortEntry. staPortAdminEdgePort	Lecture/ Ecriture	true (1), false (2)	false

Nom de zone	Variable MIB	Accès	Plage de valeurs	Valeur par défaut
STA Port Enable (Admin status)	sun...mstMgt. mstInstancePortTable. mstInstancePortEntry. mstInstancePortEnable	Lecture/ Ecriture	enabled (1), disabled (2)	enabled
STA Port Role	sun...mstMgt. mstInstancePortTable. mstInstancePortEntry. mstInstancePortPortRole	Lecture seule	disabled (1), root (2), designated (3), alternate (4), backup (5)	
STA Port Designated Root	sun...mstMgt. mstInstancePortTable. mstInstancePortEntry. mstInstancePort-DesignatedRoot	Lecture seule	Chaîne d'octets	
STA Port Forward Transitions	sun...mstMgt. mstInstancePortTable. mstInstancePortEntry. mstInstancePort-ForwardTransitions	Lecture seule	Compteur	

3.4.6.2 Configuration des paramètres d'interface pour STA

Ces paramètres s'appliquent aux interfaces sélectionnées lorsque le commutateur est défini au mode de compatibilité STP forcée (page 4-57) et RSTP.

Attributs des commandes

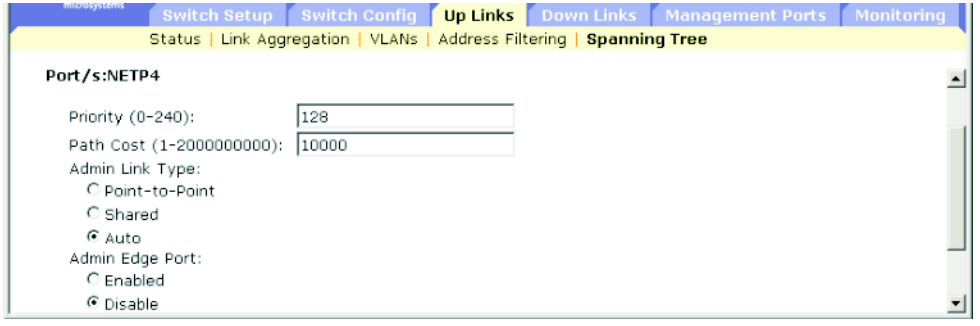
- **Priority** : Définit la priorité utilisée pour ce port dans l'algorithme Spanning Tree (STA). Si la distance à parcourir pour tous les ports sur un commutateur est identique, le port avec la priorité la plus élevée (à savoir la valeur la plus basse) est configuré comme liaison active dans le Spanning Tree. Cette fonction rend le port avec la priorité la plus élevée moins susceptible d'être bloqué si le STA détecte des boucles réseau. Si plus d'un port possède la priorité la plus élevée, le port activé est celui avec l'identificateur numérique le plus bas.
  - Valeurs par défaut : 128
  - Plage : 0-240, par incréments de 16
- **Path Cost** : Ce paramètre est utilisé par le STA pour déterminer le meilleur chemin entre les périphériques. C'est pourquoi les valeurs inférieures doivent être affectées aux ports attachés aux supports les plus rapides, et les valeurs supérieures aux ports avec les supports les plus lents. (La distance à parcourir est prioritaire sur la priorité du port).
  - Plage :
    - Ethernet : 200 000-20 000 000
    - Fast Ethernet : 20 000-2 000 000
    - Gigabit Ethernet : 2 000-200 000

- Par défaut :
  - Ethernet : semi duplex : 2 000 000 ; duplex : 1 000 000 ; groupe : 500 000
  - Fast Ethernet : semi duplex : 200 000 ; duplex : 100 000 ; groupe : 50 000
  - Gigabit Ethernet : duplex : 10 000 ; groupe : 5 000

Remarque - Lorsque la méthode est « short » (page 4-63), la distance maximale est de 65 535.

- **Admin Link Type** : Type de liaison attachée à cette interface. (Par défaut : Auto)
  - Point-par-point : Connexion à un seul autre pont.
  - Partagé : Connexion à deux ou plusieurs ponts.
  - Auto : Le commutateur détermine automatiquement si l'interface est attachée à un lien point-par-point ou à un support partagé.
- **Admin Edge Port** : Vous pouvez activer cette option si une interface est attachée à un segment LAN qui se trouve à la fin d'un LAN contenant des ponts ou sur un noeud final. Etant donné que les noeuds finaux **ne peuvent pas** provoquer de boucles de transmission, ils peuvent passer directement à l'état de transmission du Spanning Tree. Spécifier les ports de périphérie permet une convergence plus rapide pour les périphériques tels que les stations de travail ou les serveurs, conserve la base de données de transmission courante pour réduire la quantité de trames envoyées requises pour reconstruire les tables d'adressages pendant les événements de reconfiguration, ne pousse pas le Spanning Tree à initier la reconfiguration lorsque l'interface change d'état et permet également d'éviter d'autres problèmes de temporisation liés au STA. Toutefois, rappelez-vous que le port de périphérie ne doit être activé que pour les ports connectés à un périphérique de noeud final. (Par défaut : NETP0-7 : désactivé ; SNP0-15 : activé et défini avec cette valeur)

Web : Cliquez sur Up Links / Down Links=>Spanning Tree=>Spanning Tree Protocol. Pour configurer les paramètres d'interface du STP (IEEE 802.1D), cochez la case des interfaces requises et cliquez sur Configure. Ensuite, modifiez les attributs requis, et cliquez sur Save.



ILC : Cet exemple définit les attributs STP pour le port NETP5.

```
Console(config)# interface ethernet NETP5 4-74
Console(config-if)#spanning-tree port-priority 128 4-100
Console(config-if)#spanning-tree cost 19                    4-99
Console(config-if)#spanning-tree link-type auto 4-102
Console(config-if)#no spanning-tree edge-port 4-101
```

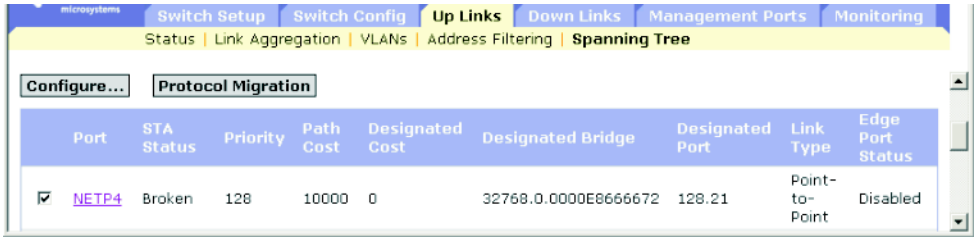
SNMP : Variables MIB équivalentes.

Nom de zone	Variable MIB	Accès	Plage de valeurs	Valeur par défaut
STA Port Priority	sun...mstMgt. mstInstancePortTable. mstInstancePortEntry. mstInstancePortPriority	Lecture/ Ecriture	Nombre entier (0-240)	128
STA Port Path Cost	sun...mstMgt. mstInstancePortTable. mstInstancePortEntry. mstInstancePortPathCost	Lecture/ Ecriture	Nombre entier (long : 1-200 000 000 ; court : 1-65,535)	page 4-107
STA Port Admin Link Type	sun...staMgt. staPortTable. staPortEntry. staPortAdmin-PointToPoint	Lecture/ Ecriture	forceTrue (0), forceFalse (1), auto (2)	auto
STA Port Admin Edge Port	sun...staMgt. staPortTable. staPortEntry. staPortAdminEdgePort	Lecture/ Ecriture	true (1), false (2)	false

3.4.6.3 Vérification de l'état du protocole STA pour les interfaces

Si, à un moment donné, le commutateur détecte des BPDU STP, y compris des BDPU Configuration ou Topology Change Notification, il définit automatiquement l'interface sélectionnée au mode compatibilité STP forcée. Toutefois, vous pouvez également utiliser le bouton Protocol Migration pour resélectionner manuellement le format BPDU approprié (compatible RSTP ou STP) à envoyer sur les interfaces sélectionnées.

Web : Cliquez sur Up Links / Down Links=>Spanning Tree=>Spanning Tree Protocol. Sélectionnez les interfaces requises, puis cliquez sur le bouton Protocol Migration.



ILC : L'exemple suivant utilise la commande de migration du protocole pour vérifier le type de message du Spanning Tree (à savoir compatible RSTP ou STP) à envoyer sur cette interface.

```
Console(config)interface ethernet NETP4
Console(config-if)#spanning-tree protocol-migration4-102
Console(config-if)#
```

SNMP : Variables MIB équivalentes.

Nom de zone	Variable MIB	Accès	Plage de valeurs	Valeur par défaut
STA Port Protocol Migration	sun...staMgt. staPortTable. staPortEntry. staPortProtocolMigration	Lecture/ Ecriture	true (1), false (2)	true

3.4.7 Filtrage du trafic depuis le port de gestion

Vous pouvez configurer le filtrage des paquets afin qu'il empêche un trafic IP spécifié d'atteindre le port de gestion interne (NETMGT) depuis les ports à liaison descendante. (Remarquez que le trafic ne peut jamais passer des ports à liaison ascendante au port de gestion.)

Utilisation de la commande

- Par défaut, le système arrête tous les paquets IP passant entre le port de gestion interne et les ports à liaison descendante. Si vous devez accéder aux serveurs Blade par le biais du port de gestion, vous devez définir un filtre autorisant les paquets spécifiés à passer entre le port de gestion et les ports à liaison descendante.
- Par défaut, le système arrête tous les paquets IP passant des ports à liaison descendante au port de gestion (NETMGT). Si les serveurs Blade doivent pouvoir accéder au réseau de gestion par le biais du port de gestion (NETMGT), vous devez définir un filtre autorisant des trames spécifiques à passer entre les ports à liaison descendante et le port de gestion.

Remarque : Aucun trafic n'est autorisé entre les ports à liaison ascendante et le port de gestion.

Attributs des commandes

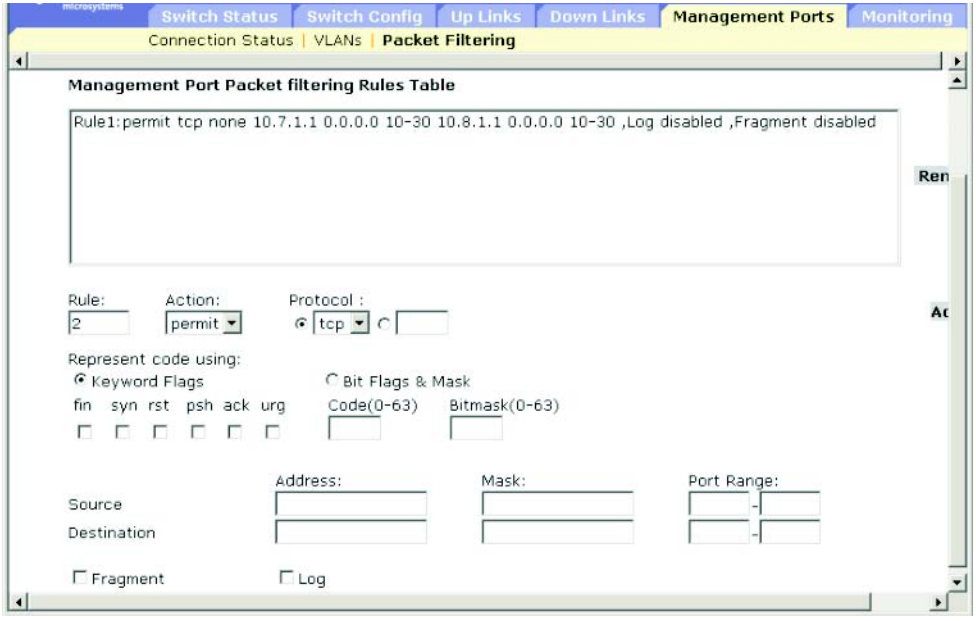
- **Rule** : Insère une règle de filtrage à l'emplacement spécifié de la table, décalant d'un rang les motifs existants à cet emplacement, ou sous celui-ci, dans la table. Un numéro de règle ne peut pas dépasser le numéro suivant disponible dans la table. Si le numéro de la règle n'est pas spécifié, un nouveau motif est joint à la fin de la table des règles. (Plage : 1-128)
- **Action** : Empêche ou autorise le passage des paquets des ports à liaison descendante au port de gestion. (Options : permit, deny)
- **Protocol** : Sélectionne un protocole (TCP, UDP, Any) ou un numéro de protocole (0-255).
- **Keyword Flags** (Séquence de code) : Indique un code à l'octet 14 de l'en-tête TCP. Vous pouvez spécifier une séquence de codes (à savoir ON en cas de sélection et OFF en cas de non-sélection). Le nom symbolique et le bit correspondant comprennent les éléments suivants :
  - **fin** (1) - Finish
  - **syn** (2) - Synchronize
  - **rst** (4)- Reset
  - **psh** (8) - Push
  - **ack** (16) - Acknowledgement
  - **urg** (32) - Urgent pointer
- **Code** : Nombre décimal (représentant une chaîne de bits) spécifiant un code à l'octet 14 de l'en-tête TCP. (Plage : 0-63)

- **Bitmask** : Nombre décimal (représentant un masque de bits) appliqué au code. Entrez un nombre décimal, où l'équivalent binaire « 1 » signifie une correspondance avec un bit et « 0 » signifie qu'un bit est ignoré. Il est possible de spécifier les bits suivants :

  32 (urg), 16 (ack), 8 (psh), 4 (rst), 2 (syn), 1 (fin)

- **Source** : Adresse source TCP/UDP, masque de réseau et plage des ports de la trame. (Plage des ports : 0-65535)
- **Destination** : adresse de destination TCP/UDP, masque de réseau et plage des ports de la balise. (Plage du port : 0-65535)
- **Fragment** : La règle ne recherche que les paquets avec le bit MF (More Fragments) actif ou avec un décalage de fragments supérieur à zéro. Si cette option n'est pas définie, la règle recherche à la fois les fragments et les paquets non fragmentés.
- **Log** : Consigne tous les paquets correspondants dans le tampon de journalisation. Le nombre maximal d'entrées enregistrées dans ce tampon est de 64. Lorsque le tampon est plein, il revient au début et écrase les entrées les plus anciennes. Remarquez que le journal est enregistré dans la RAM et qu'il s'efface lorsque le commutateur est réinitialisé.

Web : Cliquez sur Management Port=>Packet Filtering. Entrez les règles requises, puis cliquez sur Add. La règle de cet exemple autorise le trafic TCP de l'adresse source 10.7.1.1 à l'adresse de destination 10.8.1.1, à l'aide des ports TCP 10-30.



ILC : Cet exemple permet à tous les paquets de passer par le filtre en autorisant tous les types de protocoles ainsi qu'une adresse nulle et un masque de réseau tant pour l'adresse source que pour l'adresse de destination. Pour obtenir une liste complète d'exemples, reportez-vous à Section 4.3.7.8, « ip filter » à la page 4-68

```
Console(config)#ip filter permit any 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0   4-68
Console(config)#
```

SNMP : Variables MIB équivalentes.

Nom de zone	Variable MIB	Accès	Plage de valeurs	Valeur par défaut
Index	sun... securityMgt. packetFilterUnitMgt. pfuRuleTable. pfuRuleEntry. pfuRuleIndex	Aucun accès	Nombre entier (1-128)	
Action	sun... securityMgt. packetFilterUnitMgt. pfuRuleTable. pfuRuleEntry. pfuRuleAction	Lecture/ Création	permit (1), deny (2)	
Protocol	sun... securityMgt. packetFilterUnitMgt. pfuRuleTable. pfuRuleEntry. pfuRuleProtocol	Lecture/ Création	Nombre entier (0-256; 256 signifie tous les protocoles)	
Source IP Address & Bitmask	sun... securityMgt. packetFilterUnitMgt. pfuRuleTable. pfuRuleEntry. pfuRuleSrcIpAddr & pfuRuleSrcIpBitmask	Lecture/ Création	Adresse IP	
Source IP Port Range	sun... securityMgt. packetFilterUnitMgt. pfuRuleTable. pfuRuleEntry. pfuRuleSrcPortRange1 & pfuRuleSrcPortRange2	Lecture/ Création	Nombre entier (1-65536)	
Destination IP Address & Bitmask	sun... securityMgt. packetFilterUnitMgt. pfuRuleTable. pfuRuleEntry. pfuRuleDstIpAddr & pfuRuleDstIpBitmask	Lecture/ Création	Adresse IP	

Nom de zone	Variable MIB	Accès	Plage de valeurs	Valeur par défaut
Destination IP Port Range	sun... securityMgt. packetFilterUnitMgt. pfuRuleTable. pfuRuleEntry. pfuRuleDstPortRange1 & pfuRuleDstPortRange2	Lecture/ Création	Nombre entier (1-65536)	
TCP Code	sun... securityMgt. packetFilterUnitMgt. pfuRuleTable. pfuRuleEntry. pfuRuleTcpCode	Lecture/ Création	Nombre entier (0-63)	
TCP Code Bitmask	sun... securityMgt. packetFilterUnitMgt. pfuRuleTable. pfuRuleEntry. pfuRuleTcpCodeBitmask	Lecture/ Création	Nombre entier (0-63)	
Fragments	sun... securityMgt. packetFilterUnitMgt. pfuRuleTable. pfuRuleEntry. pfuRuleFragments	Lecture/ Création	enabled (1), disabled (2)	disabled
Log	sun... securityMgt. packetFilterUnitMgt. pfuRuleTable. pfuRuleEntry. pfuRuleLog	Lecture/ Création	enabled (1), disabled (2)	disabled

3.5 Surveillance du port et du trafic de gestion

Cette section décrit les fonctions de surveillance du commutateur, y compris celles permettant de mettre le trafic en miroir sur un port de surveillance à des fins d'analyse, d'afficher des statistiques réseau détaillées pour n'importe quel port ou d'afficher des statistiques clés sur le trafic SNMP passant par le port de gestion.

Remarque - Les commutateurs intégrés sur le châssis Sun Fire™ B1600 pour serveurs Blade sont chacun composés de deux puces de commutateurs reliées. Il n'est possible de mettre en miroir le trafic d'un port qu'en utilisant un autre port situé sur la même puce. Les ports NETP0, NETP1, NETP4, NETP5 ainsi que SNP8 à SNP15 se trouvent sur l'une des puces. Les ports NETP2, NETP3, NETP6, NETP7 ainsi que SNP0 à SNP7 se trouvent sur l'autre. Si vous regardez le panneau arrière de l'unité commutateur/contrôleur système, tous les ports de droite se trouvent sur une puce et tous ceux de gauche sur l'autre.)

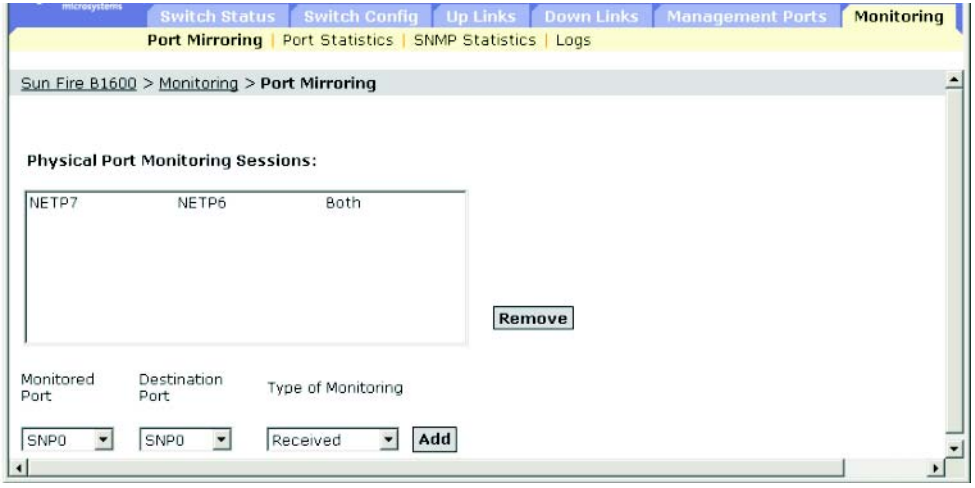
3.5.1 Configuration de la mise en miroir des ports

Vous pouvez mettre le trafic provenant d'un port source en miroir sur un port cible pour une analyse en temps réel. Vous pouvez attacher un analyseur logique ou une sonde RMON au port cible et étudier le trafic passant par le port source sans en entraver le fonctionnement.

Utilisation de la commande

- La vitesse du port de surveillance doit correspondre à la vitesse du port source ou la dépasser, sans quoi le trafic peut être interrompu sur le port de surveillance.
- Lorsque vous mettez en miroir le trafic d'un port, le port cible doit être compris dans le même VLAN que le port source.

Web : Ouvrez Monitoring=>Port Mirror. Spécifiez le port source, le type de trafic à mettre en miroir ainsi que le port de surveillance, puis cliquez sur Add.



ILC : Utilisez la commande d'interface pour sélectionner le port de surveillance, puis la commande de surveillance du port pour spécifier le port source. Remarquez que la mise en miroir par défaut sous l'ILC s'applique à la fois aux paquets reçus et transmis.

```
Console(config)#interface ethernet NETP7 4-74
Console(config-if)#port monitor ethernet NETP6 4-143
Console(config-if)#
```

SNMP : Variables MIB équivalentes.

Nom de zone	Variable MIB	Accès	Plage de valeurs	Valeur par défaut
Mirror Source Port	sun... mirrorMgt. mirrorTable.mirrorEntry. mirrorSourcePort	Non accessible	Nombre entier	
Mirror Destination Port	sun... mirrorMgt. mirrorTable.mirrorEntry. mirrorDestinationPort	Non accessible	Nombre entier	
Mirror Type	sun... mirrorMgt. mirrorTable.mirrorEntry. mirrorType	Lire/Créer	rx (1), tx (2), both (3)	both
Mirror Status	sun... mirrorMgt. mirrorTable.mirrorEntry. mirrorStatus	Lecture/ Création	valid (1), invalid (2)	

3.5.2 Affichage des statistiques du port

Vous pouvez consulter les statistiques standard relatives au trafic réseau depuis les MIB (Management Information Base) Interfaces Group et Ethernetlike, de même qu'une répartition détaillée du trafic basée sur la MIB RMON. Les interfaces et les statistiques de la MIB Ethernetlike affichent les erreurs relatives au trafic transitant par chaque port. Ces informations permettent d'identifier des problèmes potentiels avec le commutateur (tels qu'un port défaillant ou une charge anormalement élevée). Les statistiques RMON permettent d'accéder à une vaste gamme de statistiques, y compris le nombre total des différents types de trames transitant par chaque port. Toutes les valeurs affichées ont été accumulées depuis le dernier réamorçage du système et sont affichées en nombres par seconde. Par défaut, les statistiques sont actualisées toutes les 20 secondes.

Remarque - Il n'est possible d'accéder aux groupes RMON 2, 3 et 9 qu'à l'aide du SNMP.

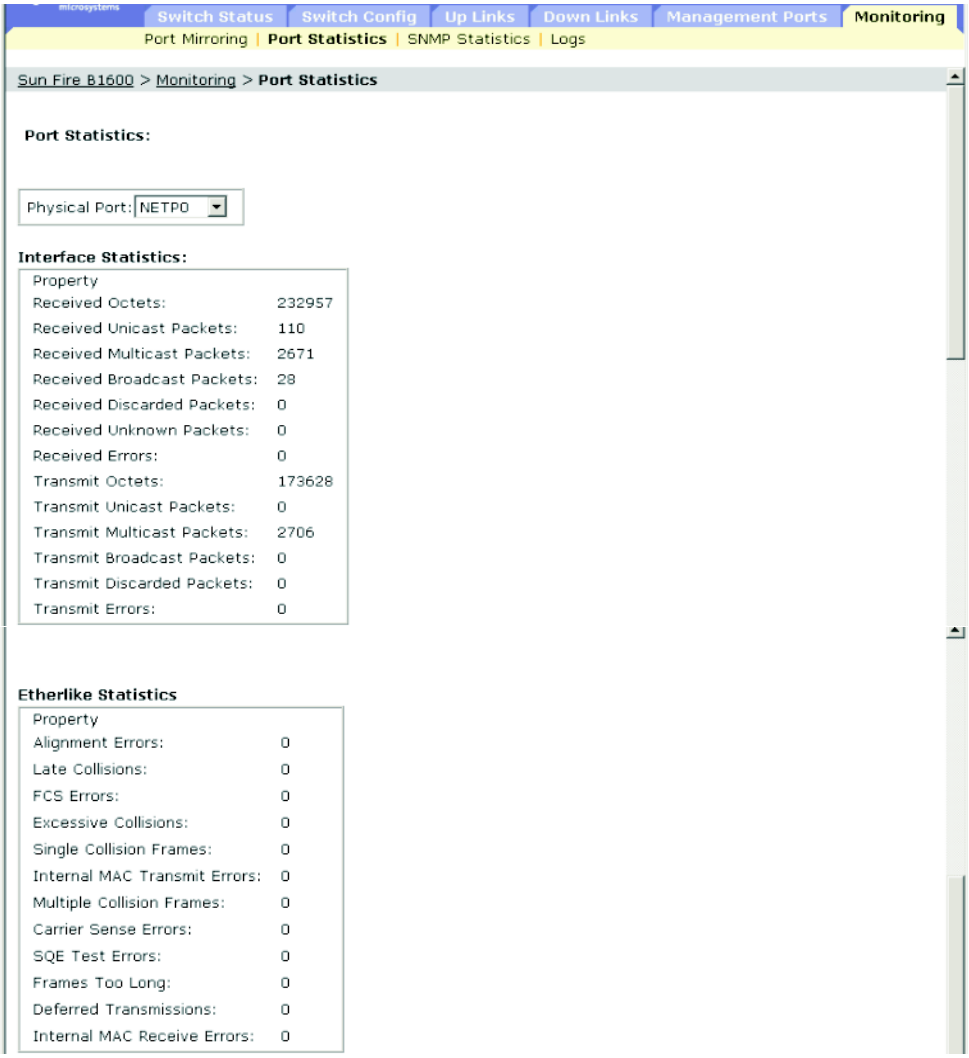
Attributs des commandes

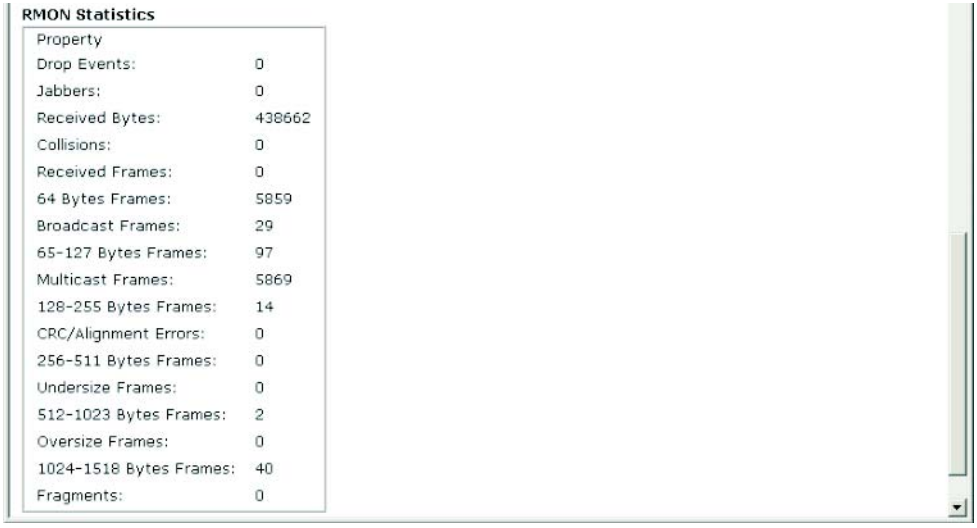
Paramètre	Description
Statistiques de l'interface	
Received Octets	Nombre total d'octets reçus sur l'interface, en ce compris les caractères de tramage.
Received Unicast Packets	Nombre de paquets du sous-réseau unidestinataire envoyés à un protocole de couche supérieure.
Received Multicast Packets	Nombre de paquets envoyés par cette sous-couche à une (sous-) couche supérieure et adressés à une adresse multidestinataire sur cette sous-couche.
Received Broadcast Packets	Nombre de paquets envoyés par cette sous-couche à une (sous-) couche supérieure et adressés à une adresse de diffusion sur cette sous-couche.
Received Discarded Packets	Nombre de paquets entrants à ignorer même si aucune erreur n'a été détectée pour empêcher qu'ils soient envoyés à un protocole de couche supérieure. L'une des raisons possibles du rejet d'un tel paquet réside dans la libération de l'espace-tampon.
Received Unknown Packets	Nombre de paquets reçus par le biais de l'interface et ignorés à cause d'un protocole inconnu ou non pris en charge.
Received Errors	Nombre de paquets entrants contenant des erreurs les empêchant d'être envoyés à un protocole de couche supérieure.
Transmit Octets	Nombre total d'octets transmis depuis l'interface, en ce compris les caractères de tramage.
Transmit Unicast Packets	Nombre total de paquets que les protocoles de niveau supérieur ont demandé à transmettre à une adresse de sous-réseau unidestinataire, en ce compris ceux qui ont été ignorés ou non envoyés.
Transmit Multicast Packets	Nombre total de paquets que les protocoles de niveau supérieur ont demandé à transmettre et qui ont été adressés à une adresse multidestinataire sur cette sous-couche, en ce compris ceux qui ont été ignorés ou non envoyés.
Transmit Broadcast Packets	Nombre total de paquets que les protocoles de niveau supérieur ont demandé à transmettre et qui ont été adressés à une adresse de diffusion sur cette sous-couche, en ce compris ceux qui ont été ignorés ou non envoyés.
Transmit Discarded Packets	Nombre de paquets sortants à ignorer même si aucune erreur n'a été détectée pour empêcher leur transmission. L'une des raisons possibles pour le rejet d'un tel paquet réside dans la libération de l'espace-tampon.
Transmit Errors	Nombre de paquets sortants qui n'ont pas pu être transmis à cause d'erreurs.

Paramètre	Description
Statistiques Etherlike	
Alignment Errors	Nombre d'erreurs d'alignement (paquets de données mal synchronisées).
Late Collisions	Nombre de détections de collisions ultérieures à 512 bits dans la transmission d'un paquet.
FCS Errors	Nombre de trames reçues sur une interface particulière et représentant un nombre entier d'octets en longueur, mais échouant au contrôle FCS. Ce nombre ne comprend pas les trames reçues avec une erreur due à une longueur excessive ou insuffisante.
Excessive Collisions	Nombre de trames dont la transmission sur une interface particulière échoue en raison de collisions excessives. Ce compteur n'augmente pas lorsque l'interface fonctionne en mode duplex.
Single Collision Frames	Nombre de trames transmises avec succès dont la transmission est entravée par une et une seule collision.
Internal MAC Transmit Errors	Nombre de trames dont la transmission sur une interface particulière échoue en raison d'une erreur interne de transmission de la sous-couche MAC.
Multiple Collision Frames	Le nombre de trames transmises avec succès dont la transmission est entravée par plus d'une collision.
Carrier Sense Errors	Nombre de fois que la condition Analyse du signal porteur a été perdue ou jamais affirmée lors des tentatives de transmission d'une trame.
SQE Test Errors	Nombre de fois que le message SQE TEST ERROR est généré par la sous-couche PLS pour une interface particulière.
Frames Too Long	Nombre de trames reçues sur une interface particulière dépassant la taille maximale autorisée.
Deferred Transmissions	Nombre de trames dont la première tentative de transmission sur une interface particulière est retardée en raison de l'occupation du support.
Internal MAC Receive Errors	Nombre de trames dont la réception sur une interface particulière échoue en raison d'une erreur interne de réception de la sous-couche MAC.
Statistiques RMON	
Drop Events	Nombre total d'événements dans lesquels des paquets ont été abandonnés en raison d'un manque de ressources.
Jabbers	Nombre total de trames reçues dont la longueur dépassait 1518 octets (à l'exclusion des bits de tramage, mais à l'inclusion des octets FCS), et comportait soit une erreur FCS soit une erreur d'alignement.

Paramètre	Description
Received Bytes	Nombre total d'octets de données reçus sur le réseau. Ces statistiques peuvent fournir une indication raisonnable de l'exploitation d'Ethernet.
Collisions	Meilleure estimation du nombre total de collisions sur ce segment Ethernet.
Received Frames	Nombre total de trames (mauvaises, diffusion et multidestinataires) reçues.
Broadcast Frames	Nombre total de bonnes trames reçues et dirigées vers l'adresse de diffusion. Remarquez que ce nombre n'inclut pas les paquets multidestinataires.
Multicast Frames	Nombre total de bonnes trames reçues et dirigées vers l'adresse multidestinataire.
CRC/Alignment Errors	Nombre d'erreurs d'alignement/CRC (erreurs FCS ou d'alignement).
Undersize Frames	Nombre total de trames reçues dont la longueur était inférieure à 64 octets (à l'exclusion des bits de tramage, mais à l'inclusion des octets FCS), et bien formées par ailleurs.
Oversize Frames	Nombre total de trames reçues dont la longueur était supérieure à 1518 octets (à l'exclusion des bits de tramage, mais à l'inclusion des octets FCS), et bien formées par ailleurs.
Fragments	Nombre total de trames reçues dont la longueur était inférieure à 64 octets (à l'exclusion des bits de tramage, mais à l'inclusion des octets FCS), et comportait soit une erreur FCS soit une erreur d'alignement.
64 Bytes Frames	Nombre total de trames (y compris les mauvais paquets) reçues et transmises dont la longueur était égale à 64 octets (à l'exclusion des bits de tramage, mais à l'inclusion des octets FCS).
Trames de 65-127 octets Trames de 128-255 octets Trames de 256-511 octets Trames de 512-1023 octets Trames de 1024-1518 octets Trames de 1519-1536 octets	Nombre total de trames (y compris les mauvais paquets) reçues et transmises dont le nombre d'octets se situe dans la plage spécifiée (à l'exclusion des bits de tramage, mais à l'inclusion des octets FCS).

Web : Cliquez sur Monitoring=>Statistics. Sélectionnez l'interface requise, puis cliquez sur Select. Vous pouvez également utiliser le bouton Refresh situé en bas de la page pour mettre l'écran à jour.





ILC : L'exemple suivant affiche les statistiques du port SNP13.

```
Console#show interfaces counters ethernet SNP134-84
Ethernet 13
 Iftable stats:
  Octets input: 868453, Octets output: 3492122
  Unicast input: 7315, Unicast output: 6658
  Discard input: 0, Discard output: 0
  Error input: 0, Error output: 0
  Unknown protos input: 0, QLen output: 0
 Extended iftable stats:
  Multi-cast input: 0, Multi-cast output: 17027
  Broadcast input: 231, Broadcast output: 7
 Ether-like stats:
  Alignment errors: 0, FCS errors: 0
  Single Collision frames: 0, Multiple collision frames: 0
  SQE Test errors: 0, Deferred transmissions: 0
  Late collisions: 0, Excessive collisions: 0
  Internal mac transmit errors: 0, Internal mac receive errors: 0
  Frame too longs: 0, Carrier sense errors: 0
 RMON stats:
  Drop events: 0, Octets: 4422579, Packets: 31552
  Broadcast pkts: 238, Multi-cast pkts: 17033
  Undersize pkts: 0, Oversize pkts: 0
  Fragments: 0, Jabbers: 0
  CRC align errors: 0, Collisions: 0
  Packet size <= 64 octets: 25568, Packet size 65 to 127 octets: 1616
  Packet size 128 to 255 octets: 1249, Packet size 256 to 511 octets: 1449
  Packet size 512 to 1023 octets: 802, Packet size 1024 to 1518 octets: 871
Console#
```

SNMP : Variables MIB équivalentes.

Nom de zone	Variable MIB	Accès	Plage
Statistiques de l'interface			
In Octets	MIB-II. interfaces.ifNumber.ifTable.ifEntry.ifInOctets	Lecture seule	Nombre entier
In Unicast Packets	MIB-II. interfaces.ifNumber.ifTable.ifEntry. ifInUcastPkts	Lecture seule	Nombre entier
In Multicast Packets	MIB-II. ifMIB.ifMIBObjects.ifXTable.ifXEntry. ifInMulticastPkts	Lecture seule	Nombre entier
In Broadcast Packets	MIB-II. ifMIB.ifMIBObjects.ifXTable.ifXEntry. ifInBroadcastPkts	Lecture seule	Nombre entier
In Discards	MIB-II. interfaces.ifTable.ifEntry.ifInDiscards	Lecture seule	Nombre entier
In Unknown Protocols	MIB-II. interfaces.ifTable.ifEntry.ifInUnknownProtos	Lecture seule	Nombre entier
In Errors	MIB-II. interfaces.ifTable.ifEntry.ifInErrors	Lecture seule	Nombre entier
Out Octets	MIB-II. interfaces.ifTable.ifEntry.ifOutOctets	Lecture seule	Nombre entier
Out Unicast Packets	MIB-II. interfaces.ifTable.ifEntry.ifOutUcastPkts	Lecture seule	Nombre entier
Out Multicast Packets	MIB-II. ifMIB.ifMIBObjects.ifXTable.ifXEntry. ifOutMulticastPkts	Lecture seule	Nombre entier
Out Broadcast Packets	MIB-II. ifMIB.ifMIBObjects.ifXTable.ifXEntry. ifOutBroadcastPkts	Lecture seule	Nombre entier
Out Discards	MIB-II. interfaces.ifTable.ifEntry.ifOutDiscards	Lecture seule	Nombre entier
Out Errors	MIB-II. interfaces.ifTable.ifEntry.ifOutErrors	Lecture seule	Nombre entier

Nom de zone	Variable MIB	Accès	Plage
Statistiques Etherlike			
Alignment Errors	MIB-II. transmission.dot3StatsTable.dot3StatsEntry. dot3StatsAlignmentErrors	Lecture seule	Nombre entier
Late Collisions	MIB-II. transmission.dot3StatsTable.dot3StatsEntry. dot3StatsLateCollisions	Lecture seule	Nombre entier
FCS Errors	MIB-II. transmission.dot3StatsTable.dot3StatsEntry. dot3StatsFCSErrors	Lecture seule	Nombre entier
Excessive Collisions	MIB-II. transmission.dot3StatsTable.dot3StatsEntry. dot3Stats-ExcessiveCollisions	Lecture seule	Nombre entier
Single Collision Frames	MIB-II. transmission.dot3StatsTable.dot3StatsEntry. dot3StatsSingleCollisionFrames	Lecture seule	Nombre entier
Internal Mac Transmit Errors	MIB-II. transmission.dot3StatsTable.dot3StatsEntry. dot3StatsInternalMacTransmitErrors	Lecture seule	Nombre entier
Multiple Collision Frames	MIB-II. transmission.dot3StatsTable.dot3StatsEntry. dot3StatsMultipleCollisionFrames	Lecture seule	Nombre entier
Carrier Sense Errors	MIB-II. transmission.dot3StatsTable.dot3StatsEntry. dot3StatsCarrierSenseErrors	Lecture seule	Nombre entier
SQE Test Errors	MIB-II. transmission.dot3StatsTable.dot3StatsEntry. dot3StatsSQETestErrors	Lecture seule	Nombre entier
Frames Too Long	MIB-II. transmission.dot3StatsTable.dot3StatsEntry. dot3StatsFrameTooLongs	Lecture seule	Nombre entier
Deferred Transmissions	MIB-II. transmission.dot3StatsTable.dot3StatsEntry. dot3StatsDeferredTransmissions	Lecture seule	Nombre entier
Internal MAC Receive Errors	MIB-II. transmission.dot3StatsTable.dot3StatsEntry. dot3StatsInternalMacReceiveErrors	Lecture seule	Nombre entier

Nom de zone	Variable MIB	Accès	Plage
Statistiques RMON			
Drop Events	MIB-II. rmon.statistics.etherStatsTable.etherStatsEntry. etherStatsDropEvents	Lecture seule	Nombre entier
Jabbers	MIB-II. rmon.statistics.etherStatsTable.etherStatsEntry. etherStatsJabbers	Lecture seule	Nombre entier
Received Octets	MIB-II. rmon.statistics.etherStatsTable.etherStatsEntry. etherStatsOctets	Lecture seule	Nombre entier
Collisions	MIB-II. rmon.statistics.etherStatsTable.etherStatsEntry. etherStatsCollisions	Lecture seule	Nombre entier
Received Packets	MIB-II. rmon.statistics.etherStatsTable.etherStatsEntry. etherStatsPkts	Lecture seule	Nombre entier
Broadcast Packets	MIB-II. rmon.statistics.etherStatsTable.etherStatsEntry. etherStatsBroadcastPkts	Lecture seule	Nombre entier
Multicast Packets	MIB-II. rmon.statistics.etherStatsTable.etherStatsEntry. etherStatsMulticastPkts	Lecture seule	Nombre entier
CRC/Alignment Errors	MIB-II. rmon.statistics.etherStatsTable.etherStatsEntry. etherStatsCRCAlignErrors	Lecture seule	Nombre entier
Undersize Packets	MIB-II. rmon.statistics.etherStatsTable.etherStatsEntry. etherStatsUndersizePkts	Lecture seule	Nombre entier
Oversize Packets	MIB-II. rmon.statistics.etherStatsTable.etherStatsEntry. etherStatsOversizePkts	Lecture seule	Nombre entier
Fragments	MIB-II. rmon.statistics.etherStatsTable.etherStatsEntry. etherStatsFragments	Lecture seule	Nombre entier
64 Bytes Frames	MIB-II. rmon.statistics.etherStatsTable.etherStatsEntry. etherStatsPkts64Octets	Lecture seule	Nombre entier
X-**Y** Byte Frames	MIB-II. rmon.statistics.etherStatsTable.etherStatsEntry. etherStatsPkts**X**to**Y**Octets	Lecture seule	Nombre entier

3.5.3 Affichage des statistiques SNMP

Vous pouvez afficher les principales statistiques concernant le trafic SNMP transitant par le port de gestion. Ces informations permettent de résoudre les erreurs SNMP ou d'afficher le volume global du trafic SNMP traité par le commutateur, de même que toute tentative illégale visant à accéder au commutateur via SNMP.

Attributs des commandes

Paramètre	Description
SNMP packets input	
SNMP packets input	Nombre total de messages remis à l'entité SNMP par le service de transfert.
Bad SNMP version errors	Nombre total de messages SNMP remis à l'entité du protocole SNMP et destinés à une version SNMP non prise en charge.
Unknown community name	Nombre total de messages SNMP remis à l'entité du protocole SNMP et utilisant un nom de communauté SNMP inconnu de ladite entité.
Illegal operation for community name supplied	Nombre total de messages SNMP remis à l'entité du protocole SNMP et représentant une opération SNMP non autorisée par la communauté SNMP nommée dans le message.
Encoding errors	Nombre total d'erreurs ASN.1 ou BER rencontrées par l'entité du protocole SNMP lors du décodage des messages SNMP reçus.
Number of requested variables	Nombre total d'objets MIB récupérés avec succès par l'entité du protocole SNMP à la suite de la réception de PDU SNMP valables Get-Request et Get-Next.
Number of altered variables	Nombre total d'objets MIB modifiés avec succès par l'entité du protocole SNMP à la suite de la réception de PDU SNMP valables Set-Request.
Get-request PDUs	Nombre total de PDU SNMP Get-Request acceptés et traités par l'entité du protocole SNMP.
Get-next PDUs	Nombre total de PDU SNMP Get-Next acceptés et traités par l'entité du protocole SNMP.
Set-request PDUs	Nombre total de PDU SNMP Set-Request acceptés et traités par l'entité du protocole SNMP.

Paramètre	Description
SNMP packets output	
SNMP packets output	Nombre total de messages SNMP transmis par l'entité SNMP au service de transfert.
Too big errors	Nombre total de PDU SNMP remis à l'entité du protocole SNMP et dont le statut en matière d'erreurs est « tooBig ».
No such name errors	Nombre total de PDU SNMP remis à l'entité du protocole SNMP et dont le statut en matière d'erreurs est « noSuchName ».
Bad values errors	Nombre total de PDU SNMP remis à l'entité du protocole SNMP et dont le statut en matière d'erreurs est « badValue ».
General errors	Nombre total de PDU SNMP remis à l'entité du protocole SNMP et dont le statut en matière d'erreurs est « genErr ».
Response PDUs	Nombre total de PDU SNMP Get-Response générés par l'entité du protocole SNMP.
Trap PDUs	Nombre total de PDU SNMP Trap générés par l'entité du protocole SNMP.

Web : Cliquez sur Monitoring=>SNMP Statistics. Vous pouvez également utiliser le bouton Refresh situé en bas de la page pour mettre l'écran à jour.

ILC : Cet exemple affiche les statistiques SNMP pour le commutateur.

```
Console#show snmp4-52

SNMP traps:
 Authentication: enable
   Link-up-down: enable

SNMP communities:
   1. private, and the privilege is read/write
   2. public, and the privilege is read-only

11 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    8 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    1 Number of altered variables
    0 Get-request PDUs
    0 Get-next PDUs
    3 Set-request PDUs
11 SNMP packets output
    0 Too big errors
    0 No such name errors
    0 Bad values errors
    2 General errors
    3 Response PDUs
    0 Trap PDUs

SNMP logging: disabled
Console#
```

SNMP : Variables MIB équivalentes.

Nom de zone	Variable MIB	Accès	Plage
SNMP packets input			
In Packets	MIB-II.snmp.snmpInPkts	Lecture seule	Nombre entier
In Bad Versions	MIB-II.snmp.snmpInBadVersions	Lecture seule	Nombre entier
In Bad Community Names	MIB-II.snmp.snmpInBadCommunityNames	Lecture seule	Nombre entier
In Bad Community Uses	MIB-II.snmp.snmpInBadCommunityUses	Lecture seule	Nombre entier

Nom de zone	Variable MIB	Accès	Plage
In ASN Parse Errors	MIB-II.snmp.snmpInASNParseErrs	Lecture seule	Nombre entier
In Total Request Variables	MIB-II.snmp.snmpInTotalReqVars	Lecture seule	Nombre entier
In Total Set Variables	MIB-II.snmp.snmpInTotalSetVars	Lecture seule	Nombre entier
In Get Requests	MIB-II.snmp.snmpInGetRequests	Lecture seule	Nombre entier
In Get Nexts	MIB-II.snmp.snmpInGetNexts	Lecture seule	Nombre entier
In Set Requests	MIB-II.snmp.snmpInSetRequests	Lecture seule	Nombre entier
Silent Drops	MIB-II.snmp.snmpSilentDrops	Lecture seule	Nombre entier
Proxy Drops	MIB-II.snmp.snmpProxyDrops	Lecture seule	Nombre entier
SNMP packets output			
Out Packets	MIB-II.snmp.snmpOutPkts	Lecture seule	Nombre entier
Out Too Bigs	MIB-II.snmp.snmpOutTooBigs	Lecture seule	Nombre entier
Out No Such Names	MIB-II.snmp.snmpOutNoSuchNames	Lecture seule	Nombre entier
Out Bad Values	MIB-II.snmp.snmpOutBadValues	Lecture seule	Nombre entier
Out General Errors	MIB-II.snmp.snmpOutGenErrs	Lecture seule	Nombre entier
Out Get Responses	MIB-II.snmp.snmpOutGetResponses	Lecture seule	Nombre entier
Out Traps	MIB-II.snmp.snmpOutTraps	Lecture seule	Nombre entier

3.5.4 Configuration des journaux de messages

Vous pouvez limiter les messages système enregistrés dans la mémoire du commutateur sur la base de leur gravité.

Attributs des commandes

- **Enable Logging** : Active la journalisation des messages de déboguage ou d'erreur dans la mémoire du commutateur. (Par défaut : désactivé)
- **Logging Level** : Limite les messages système enregistrés dans la mémoire du commutateur sur la base de leur gravité. Remarquez que les messages enregistrés comprennent le niveau sélectionné jusqu'au niveau 0. (Plage : 7-0 ; Par défaut - Flash : 3-0, RAM : 7-0)

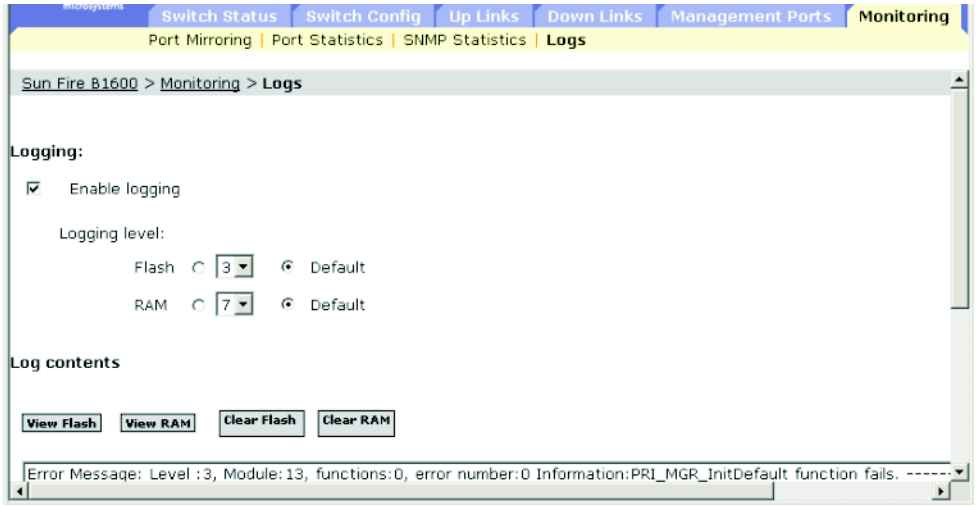
TABLEAU 3-1 Niveaux d'erreur

Argument de niveau	Niveau	Description
debugging	7	Messages de déboguage
informational	6	Messages d'information uniquement (à savoir toutes les interruptions)
notifications	5	Condition normale mais importante, telle qu'un démarrage à froid (« cold start »)
warnings	4	Conditions d'avertissement (par exemple, résultat « false », résultat inattendu)
errors	3	Conditions d'erreur (p.ex., saisie non valable, valeur par défaut utilisée)
critical	2	Conditions critiques (p.ex., allocation de mémoire ou erreur de mémoire libre - ressources épuisées)
alerts	1*	Action immédiate requise
emergencies	0*	Système inutilisable

* Il n'existe aucun message d'erreur de niveau 0 ou 1 pour la version courante du microprogramme.

- **Log contents** : Inclut des boutons vous permettant de répertorier tous les messages système ou événement enregistrés dans la mémoire Flash ou RAM, ainsi que d'effacer les messages consignés dans la mémoire Flash (à savoir la mémoire non volatile conservée après une réinitialisation du système) ou dans la RAM (à savoir la « random access memory » perdue à la réinitialisation du système).

Web : Cliquez sur Monitoring=>Logs. Activez la journalisation, cliquez sur Flash ou sur RAM, sélectionnez le niveau des messages à journaliser (niveau sélectionné jusqu'au niveau 0), puis cliquez sur Save Changes. Cliquez sur View Flash ou View RAM pour mettre à jour les messages affichés.



ILC : Cet exemple active la journalisation, définit les messages enregistrés dans la mémoire Flash au niveau 3 (à savoir « errors »), puis affiche les messages enregistrés dans la mémoire Flash.

```
Console(config)#logging on4-30
Console(config)#logging history flash 3                    4-31
Console#show logging flash4-33
Syslog logging: Enable
History logging in FLASH: level errors
[0] 0:0:5 1/1/1
   "PRI_MGR_InitDefault function fails."
   level: 3, module: 13, function: 0, and event no.: 0
Console#
```

SNMP : Variables MIB équivalentes.

Nom de zone	Variable MIB	Accès	Plage de valeurs	Valeur par défaut
Log Status	sun... sysLogMgt. sysLogStatus	Lecture/ Ecriture	enabled (1), disabled (2)	
History Flash Level	sun... sysLogMgt. sysLogStatus.sysLog.HistoryFlashLevel	Lecture/ Ecriture	Nombre entier (0-7)	
History RAM Level	sun... sysLogMgt. sysLogStatus.sysLog.HistoryRAMLevel	Lecture/ Ecriture	Nombre entier (0-7)	
Log Messages	*Non défini*			

CHAPITRE **4**

Référence de la ligne de commande

Ce chapitre décrit l'utilisation de l'interface de ligne de commande (ILC).

4.1 Utilisation de l'interface de ligne de commande

4.1.1 Accès à l'ILC

Lorsque vous ouvrez l'interface de gestion du commutateur par le biais d'une connexion directe au port console du serveur ou d'une connexion Telnet, vous pouvez gérer le commutateur en entrant les mots-clés et paramètres de commande à l'invite. L'utilisation de l'interface de ligne de commande (ILC) du commutateur ressemble fortement à la saisie de commande dans un système UNIX.

4.1.1.1 Connexion à la console

Pour accéder au commutateur par le biais du port console, procédez comme suit :

1. A l'invite de la console, entrez vos nom d'utilisateur et mot de passe. (Les noms d'utilisateur par défaut sont « admin » et « guest », avec les mots de passe correspondants « admin » et « guest ».) Lorsque vous entrez le nom d'utilisateur et le mot de passe de l'administrateur, l'ILC affiche l'invite « Console# » et passe en mode d'accès privilégié (Privileged Exec). Par contre, si vous saisissez le nom d'utilisateur et le mot de passe « guest », l'ILC affiche l'invite « Console> » et passe en mode d'accès normal (Normal Exec).
2. Entrez les commandes requises pour exécuter les tâches souhaitées.

3. Lorsque vous avez terminé, quittez la session à l'aide de la commande « quit » ou « exit ».

Lorsque vous vous connectez au système par le biais du port console, l'écran de connexion s'affiche :

```
User Access Verification

Username: admin
Password:

      CLI session with the Sun Fire B1600 is opened.
      To end the CLI session, enter [Exit].

Console#
```

4.1.1.2 Connexion Telnet

Telnet opère par le biais du protocole de transfert IP. Dans cet environnement, la station de gestion et les périphériques réseau à gérer via le réseau doivent posséder une adresse IP valable. Pour être valable, une adresse IP doit se composer de quatre nombres, de 0 à 255, séparés par des points. Chaque adresse comporte une portion réseau et une portion hôte. Par exemple, l'adresse IP 10.1.0.1 se subdivise en une portion réseau (10.1.0) et une portion hôte (1).

Remarque - Par défaut, l'adresse IP de ce commutateur n'est pas attribuée. Le port de gestion (NETMGT) est attribué au VLAN 2. Ce port ne peut pas être attribué à un VLAN contenant des ports à liaison ascendante ou à liaison descendante.

Pour accéder au commutateur par le biais d'une session Telnet, vous devez d'abord définir l'adresse IP de celui-ci, puis la passerelle par défaut si vous gérez le commutateur depuis un autre sous-réseau IP. Par exemple,

```
Console(config)#interface vlan 2
Console(config-if)#ip address 10.1.0.1 255.255.255.0
Console(config-if)#exit
Console(config)#ip default-gateway 10.1.0.254
```

Si le réseau de votre entreprise est connecté à un autre réseau extérieur à votre bureau ou à Internet, vous devez demander une adresse IP enregistrée. Toutefois, si vous êtes raccordé à un réseau isolé, vous pouvez utiliser toute adresse IP conforme à la politique réseau de votre site.

Une fois une adresse IP configurée pour le commutateur, vous pouvez ouvrir une session Telnet de la manière suivante :

1. Depuis l'hôte distant, entrez la commande Telnet et l'adresse IP du périphérique auquel vous souhaitez accéder.
2. A l'invite, entrez vos nom d'utilisateur et mot de passe système. L'ILC affiche l'invite « Vty-0# » pour l'administrateur afin de montrer que vous utilisez le mode d'accès privilégié (à savoir Privileged Exec) ou « Vty-0> » pour l'utilisateur afin de montrer que vous travaillez en mode d'accès normal (à savoir Normal Exec).
3. Entrez les commandes requises pour exécuter les tâches souhaitées.
4. Lorsque vous avez terminé, quittez la session à l'aide de la commande « quit » ou « exit ».

Une fois la commande Telnet saisie, l'écran de connexion s'affiche :

```
Username: admin
Password:

      CLI session with the Sun Fire B1600 is opened.
      To end the CLI session, enter [Exit].

Vty-0#
```

Remarque - Vous pouvez ouvrir jusqu'à quatre sessions sur le périphérique via Telnet.

4.1.2 Saisie des commandes

Cette section décrit la procédure de saisie de commandes dans l'ILC.

4.1.2.1 Mots-clés et arguments

Une commande ILC se compose d'une série de mots-clés et d'arguments. Les mots-clés identifient une commande, alors que les arguments spécifient les paramètres de configuration. Par exemple, dans la commande « show interfaces status ethernet SNP5 », **show interfaces** et **status** sont des mots-clés, **ethernet** est un argument spécifiant le type d'interface, et **SNP5** indique le port.

Vous pouvez entrer les commandes de la manière suivante :

- Pour entrer une commande simple, entrez le mot-clé correspondant.

- Pour entrer plusieurs commandes, entrez chacune d'entre elles dans l'ordre requis. Par exemple, pour activer le mode de commande « Privileged Exec » et afficher la configuration de démarrage, entrez :

  ```
  Console>enable
  Console#show startup-config
  ```

- Pour entrer des commandes requérant des paramètres, entrez les paramètres requis après le mot-clé de la commande. Par exemple, pour définir un mot de passe pour l'administrateur, entrez :

  ```
  Console(config)#username admin password 0 smith
  ```

4.1.2.2 Abréviation minimale

L'ILC accepte un nombre minimum de caractères qui identifient une commande de manière unique. Par exemple, la commande « logging history » peut être entrée sous la forme suivante : **logging h**. Si une entrée est ambiguë, le système vous invite à poursuivre la saisie.

4.1.2.3 Terminaison de la commande

Si vous terminez la saisie avec la touche Tab, l'ILC affiche les caractères restants d'un mot-clé saisi partiellement jusqu'au point où survient une ambiguïté. Dans l'exemple « logging history », si vous tapez **log** suivi d'une tabulation, l'ILC affiche la commande jusqu'à « **logging** ».

4.1.2.4 Obtention d'aide concernant les commandes

Vous pouvez consulter une brève description du système d'aide en entrant la commande **help**. Vous pouvez également visualiser la syntaxe des commandes en sélectionnant le caractère « ? » permettant de consulter mots-clés et paramètres.

4.1.2.5 Affichage des commandes

Si vous entrez « ? » à l'invite de la commande, le système affiche le premier niveau des mots-clés de la classe de commandes courante (Normal Exec ou Privileged Exec) ou de la classe de configuration (Global, Interface, Line ou VLAN Database). Vous pouvez également afficher une liste des mots-clés valables pour une commande spécifique. Par exemple, la commande « **show ?** » affiche une liste des commandes d'affichage possibles :

```
Console#show ?
  bridge-ext         Bridge extend information
  garp               Garp property
  gvrp               Show gvrp information of interface
  history            Information of history
  interfaces         Information of interfaces
  ip                 Ip
  line               TTY line information
  logging            Show the contents of logging buffers
  mac-address-table  Set configuration of the address table
  map                Map priority
  port               Characteristics of the port
  queue              Information of priority queue
  radius-server      Radius server information
  running-config     The system configuration of running
  snmp               SNMP statistics
  spanning-tree      Specify spanning-tree
  startup-config     The system configuration of starting up
  system             Information of system
  tacacs-server      Login by tacacs server
  users              Display information about terminal lines
  version            System hardware and software status
  vlan               Switch VLAN Virtual Interface
Console#show
```

La commande « show interfaces ? » affiche les informations suivantes :

```
Console>show interfaces ?
  counters    Information of interfaces counters
  status      Information of interfaces status
  switchport  Information of interfaces switchport
```

4.1.2.6 Recherche de mots-clés partiels

Si vous terminez un mot-clé partiel par un point d'interrogation, le système propose les différentes solutions correspondant aux lettres initiales. (Rappelez-vous de ne pas laisser d'espace entre la commande et le point d'interrogation). Par exemple « s? » affiche tous les mots-clés commençant par « s ».

```
Console#show s?
snmp            spanning-tree   startup-config  system
```

4.1.2.7 Annulation d'une commande

Pour de nombreuses commandes de configuration, vous pouvez entrer le mot-clé préfixe « **no** » pour annuler l'effet d'une commande ou réinitialiser la configuration à sa valeur par défaut. Par exemple, la commande **logging** journalise les messages système sur un serveur hôte. Pour désactiver la journalisation, spécifiez la commande **no logging**. Le présent manuel décrit l'annulation de toutes les commandes applicables.

4.1.2.8 Utilisation de l'historique des commandes

L'ILC gère un historique des commandes saisies. Vous pouvez faire défiler l'historique des commandes en appuyant sur la flèche dirigée vers le haut. Toute commande affichée dans l'historique peut être exécutée une nouvelle fois telle quelle ou d'abord modifiée, puis exécutée.

La commande **show history** affiche une liste plus longue des commandes récemment exécutées.

4.1.2.9 Explication des modes de commande

La commande définie est divisée en classes Exec et Configuration. Les commandes Exec affichent généralement des informations sur l'état du système ou réinitialisent les compteurs statistiques. Par ailleurs, les commandes de configuration modifient les paramètres d'interface et activent certaines fonctions de commutation. Ces classes se divisent à leur tour en différents modes. Les commandes disponibles dépendent du mode sélectionné. Vous pouvez toujours entrer un point d'interrogation « ? » à l'invite pour afficher une liste des commandes disponibles pour le mode courant. Les classes de commande et les modes associés sont présentés dans le tableau suivant :

Classe	Mode
Exec	Normal
	Privileged
Configuration*	Global
	Interface
	Line
	VLAN Database

* Vous devez être en mode « Privileged Exec » pour pouvoir accéder à l'un des modes de configuration.

4.1.2.10 Commandes Exec

Lorsque vous ouvrez une nouvelle session de console sur le commutateur avec le nom d'utilisateur et le mot de passe « guest », le système passe en mode de commande « Normal Exec » (ou mode « guest ») et affiche l'invite de commande « Console> ». Seul un nombre limité de commandes sont disponibles dans ce mode. Vous ne pouvez accéder à toutes les commandes que depuis le mode de commande « Privileged Exec » (ou mode administrateur). Pour passer en mode « Privileged Exec », ouvrez une nouvelle session de console avec les nom d'utilisateur et mot de passe admin. Le système affiche désormais l'invite de commande « Console# ». Vous pouvez également passer en mode « Privileged Exec » depuis le mode « Normal Exec », en entrant la commande **enable**, suivie du mot de passe correspondant « super » (page 4-27).

Pour passer en mode « Privileged Exec », entrez les nom d'utilisateur et mot de passe suivants :

```
Username: admin
Password: [admin login password]

      CLI session with the Sun Fire B1600 is opened.
      To end the CLI session, enter [Exit].

Console#
```

```
Username: guest
Password: [guest login password]

      CLI session with the Sun Fire B1600 is opened.
      To end the CLI session, enter [Exit].

Console>enable
Password: [privileged level password]
Console#
```

4.1.2.11 Commandes de configuration

Les commandes de configuration sont des commandes du niveau « Privileged » utilisées pour modifier les paramètres du commutateur. Ces commandes ne modifient que la configuration courante et ne sont pas enregistrées lorsque le commutateur est réamorcé. Pour enregistrer la configuration courante dans la mémoire non volatile, utilisez la commande **copy running-config startup-config**.

Les commandes de configuration sont organisées dans les modes suivants :

- Global Configuration : Ces commandes modifient la configuration au niveau du système et comprennent des commandes telles que **hostname** et **snmp-server community**.
- Interface Configuration : Ces commandes modifient la configuration du port telle que **speed-duplex** et **negotiation**.
- Line Configuration : Ces commandes modifient la configuration du port console et de Telnet et comprennent des commandes telles que **exec-timeout** et **silent-time**.
- VLAN Configuration : Cette option comprend la commande permettant de créer des groupes de VLAN.

Pour passer en mode « Global Configuration », entrez la commande **configure** en mode « Privileged Exec ». L'invite système affiche « Console(config)# », vous donnant un accès privilégié à toutes les commandes Global Configuration.

```
Console#configure
Console(config)#
```

Pour passer aux autres modes, entrez l'une des commandes suivantes à l'invite de configuration. La commande **exit** vous permet de retourner au mode Configuration et la commande **end** de retourner au « Privileged Exec ».

Mode	Commande	Invite	Voir page
Interface	interface {ethernet *port* | port-channel *id* | vlan *id*}	Console(config-if)#	4-74
Line	line {console | vty}	Console(config-line)#	4-55
VLAN	vlan database	Console(config-vlan)	4-106

Par exemple, vous pouvez utiliser les commandes suivantes pour passer en mode de configuration d'interface, puis revenir au mode « Privileged Exec ».

```
Console(config)#interface ethernet SNP5
.
.
.
Console(config-if)#exit
Console(config)
```

4.1.2.12 Traitement de la ligne de commande

Les commandes ne respectent pas la casse. Vous pouvez abréger les commandes et les paramètres pour autant qu'ils contiennent assez de lettres pour les différencier d'autres options actuellement disponibles. Vous pouvez utiliser la touche Tab pour compléter des commandes partielles ou entrer une commande partielle suivie du caractère « ? » pour afficher une liste des correspondances éventuelles. Il est également possible d'utiliser les touches d'édition suivantes pour le traitement de la ligne de commande :

Touches	Fonction
Ctrl-A	Déplace le pointeur au début de la ligne de commande.
Ctrl-B	Déplace le pointeur d'un caractère vers la gauche.
Ctrl-E	Déplace le pointeur à la fin de la ligne de commande.
Ctrl-F	Déplace le pointeur d'un caractère vers la droite.
Ctrl-P	Affiche la dernière commande.
Ctrl-U	Efface toute la ligne.
Ctrl-W	Efface le dernier mot entré.
Touche Suppr ou Espace arrière	Efface une erreur lorsque vous entrez une commande

4.2 Groupes de commandes

Les commandes système peuvent être classées dans les groupes fonctionnels présentés ci-dessous.

Groupe de commandes	Description	Page
General	Commandes de base permettant de passer au mode d'accès privilégié, de redémarrer le système ou de quitter l'ILC.	4-12
Flash/File	Commandes permettant de gérer les fichiers images du code ou les fichiers de configuration du commutateur.	4-18
System Management	Commandes contrôlant les journaux système, les mots de passe système, le nom d'utilisateur, les options de gestion du navigateur et diverses autres informations sur le système.	4-24
Authentication	Commandes permettant de configurer l'authentification à la connexion sur la base des méthodes locale, RADIUS ou TACACS.	4-41
SNMP	Commandes permettant d'activer les interruptions en cas d'échec de l'authentification ; de configurer les chaînes de communauté ainsi que les gestionnaires d'interruptions.	4-48
Line	Commandes permettant de définir les options de connexion pour le port série et Telnet, y compris la vérification du mot de passe, le mot de passe de ligne et le délai de temporisation de la console.	4-54
IP	Commandes permettant de configurer l'adresse IP et la passerelle permettant l'accès à des fins de gestion, d'afficher la passerelle par défaut ou de vérifier la connexion d'un périphérique spécifié.	4-62
Interface	Commandes permettant de configurer les paramètres de connexion pour tous les ports Ethernet, les liaisons groupées et les VLAN.	4-73
Address Table	Commandes permettant de configurer la table d'adressage permettant de filtrer des adresses spécifiées, d'afficher des entrées courantes, d'effacer la table ou de définir le délai d'obsolescence.	4-86
Port Security	Commandes permettant de configurer des adresses sécurisées pour un port.	4-90
Spanning Tree	Commandes permettant de configurer les paramètres du Spanning Tree pour le commutateur.	4-92
VLAN	Commandes permettant de configurer les paramètres du VLAN et de définir l'appartenance d'un port aux groupes de VLAN.	4-105

Groupe de commandes	Description	Page
GVRP and Bridge Extension	Commandes permettant de configurer les paramètres GVRP autorisant l'apprentissage automatique des VLAN ; d'afficher la configuration de la MIB (Management Information Base) Extension Bridge.	4-115
IGMP Snooping	Commandes permettant de configurer le filtrage multidestinataire IGMP, l'éligibilité du requêteur et les paramètres de requête ainsi que de spécifier les ports attachés à un routeur multidestinataire.	4-121
Priority	Commandes permettant de définir la priorité du port pour les trames non marquées, le poids relatif de chaque file d'attente avec priorité et le nombre maximal de files d'attente activées ; de définir la priorité la plus élevée entre le priorité IP et DSCP.	4-132
Mirror Port	Commandes permettant de mettre des données en miroir sur un autre port à des fins d'analyse sans affecter le débit de données ou les performances du port surveillé.	4-143
Port Trunking and LACP	Commandes permettant de rassembler plusieurs ports en un seul groupe logique de manière statique et de configurer le protocole LACP (Link Aggregation Control Protocol) pour les groupes de ports.	4-145

Le mode d'accès affiché dans les tableaux suivants est indiqué par les abréviations suivantes :

NE (Normal Exec)
PE (Privileged Exec)
GC (Global Configuration)
IE (Interface Configuration)
LC (Line Configuration)
VC (VLAN Database Configuration)

4.3 Description détaillée des commandes

4.3.1 Commandes générales

Commande	Fonction	Mode	Page
enable	Active le mode privilégié	NE	4-13
disable	Retourne au mode normal depuis le mode privilégié	PE	4-14
configure	Active le mode de configuration global (Global Configuration)	PE	4-14
show history	Affiche le tampon contenant l'historique des commandes	NE, PE	4-15
reload	Redémarre le système	PE	4-16
end	Retourne au mode « Privileged Exec »	GC, IC, LC, VC	4-16
exit	Retourne au mode de configuration précédent ou quitte l'ILC	indifférent	4-17
quit	Quitte une session ILC	NE, PE	4-17
help	Affiche l'aide à l'utilisation	indifférent	NA
?	Affiche les options relatives à la terminaison des commandes (selon le contexte)	indifférent	NA

4.3.1.1 enable

Cette commande permet d'activer le mode « Privileged Exec ». Dans ce mode, d'autres commandes sont disponibles, et certaines commandes proposent davantage d'informations. Voir « Explication des modes de commande », page 4-7.

Syntaxe

enable [*level*]

level : Mode privilégié de connexion au périphérique.
Le périphérique possède deux niveaux d'accès : 0: Normal Exec,
15: Privileged Exec. Entrez le niveau 15 pour accéder au mode « Privileged Exec ».

Configuration par défaut

Niveau 15

Mode de commande

Normal Exec

Utilisation de la commande

- « super » est le mot de passe par défaut requis pour passer du mode de commande « Normal Exec » à « Privileged Exec ». (Pour définir le mot de passe, consultez la commande **enable password** à la page 4-27.)
- Le caractère « # » est ajouté à la fin de l'invite pour indiquer que le système est en mode d'accès privilégié.

Exemple

```
Console>enable
Password: [privileged level password]
Console#
```

Commandes associées

disable (4-14)
enable password (4-27)

4.3.1.2 disable

Cette commande permet de retourner au mode « Normal Exec ». En mode d'accès normal, vous ne pouvez consulter que des informations de base sur la configuration du commutateur ou les statistiques Ethernet. Pour avoir accès à toutes les commandes, vous devez utiliser le mode privilégié. Voir « Explication des modes de commande », page 4-7.

Configuration par défaut

Aucune

Mode de commande

Privileged Exec

Utilisation de la commande

Le caractère « > » est ajouté à la fin de l'invite pour indiquer que le système est en mode d'accès normal.

Exemple

```
Console#disable
Console>
```

Commandes associées

enable (4-13)

4.3.1.3 configure

Cette commande permet d'activer le mode « Global Configuration ». Vous devez passer à ce mode pour modifier les paramètres du commutateur. Vous devez également y entrer pour activer certains autres modes de configuration, et notamment Interface Configuration, Line Configuration et VLAN Database Configuration. Voir « Explication des modes de commande », page 4-7.

Configuration par défaut

Aucune

Mode de commande

Privileged Exec

Exemple

```
Console#configure
Console(config)#
```

Commandes associées

end (4-16)

4.3.1.4 show history

Cette commande permet d'afficher le contenu du tampon de l'historique des commandes.

Configuration par défaut

Aucune

Mode de commande

Normal Exec, Privileged Exec

Utilisation de la commande

La taille du tampon de l'historique est fixée à 10 commandes Exécution et 10 commandes Configuration.

Exemple

Dans cet exemple, la commande show history énumère le contenu du tampon de l'historique des commandes :

```
Console#show history
Execution command history:
 2 config
 1 show history

Configuration command history:
 4 interface vlan 1
 3 exit
 2 interface vlan 1
 1 end

Console#
```

La commande **!** répète les commandes de l'historique des commandes Execution lorsque vous êtes en mode « Normal Exec » ou « Privileged Exec » et celles de l'historique des commandes Configuration lorsque vous êtes dans l'un des modes de configuration. Dans l'exemple, la commande **!2** répète la deuxième commande du tampon historique Execution (**config**).

```
Console#!2
Console#config
Console(config)#
```

4.3.1.5 reload

Cette commande permet de redémarrer le système.

Remarque - Lorsque le système est redémarré, il exécute toujours un test à la mise sous tension. Il conserve également toutes les informations de configuration enregistrées dans la mémoire non volatile par la commande **copy running-config startup-config**.

Configuration par défaut

Aucune

Mode de commande

Privileged Exec

Utilisation de la commande

La commande réinitialise l'ensemble du système.

Exemple

L'exemple suivant montre comment réinitialiser le commutateur :

```
Console#reload
System will be restarted, continue <y/n>? y
```

4.3.1.6 end

Cette commande permet de retourner au mode « Privileged Exec ».

Configuration par défaut

Aucune

Mode de commande

Global Configuration, Interface Configuration, Line Configuration, VLAN Database Configuration, Router Configuration

Exemple

L'exemple suivant montre comment retourner au mode « Privileged Exec » depuis le mode « Interface Configuration » :

```
Console(config-if)#end
Console#
```

4.3.1.7 exit

Cette commande permet de retourner au mode de configuration précédent ou de quitter le programme de configuration.

Configuration par défaut

Aucune

Mode de commande

Tous

Exemple

L'exemple suivant montre comment retourner au « Privileged Exec » depuis le mode « Global Configuration » avant de quitter la session de l'ILC :

```
Console(config)#exit
Console#exit

Press ENTER to start session

User Access Verification

Username:
```

4.3.1.8 quit

Cette commande permet de quitter la session de l'ILC.

Configuration par défaut

Aucune

Mode de commande

Normal Exec, Privileged Exec

Utilisation de la commande

Les commandes **quit** et **exit** permettent toutes les deux de quitter le programme de configuration.

Exemple

L'exemple suivant montre comment quitter une session de l'ILC :

```
Console#quit

Press ENTER to start session

User Access Verification

Username:
```

4.3.2 Commandes Flash/File

Ces commandes permettent de gérer le code système ou les fichiers de configuration.

Commande	Fonction	Mode	Page
copy	Copie une image code ou une configuration commutateur vers ou depuis la mémoire Flash ou un serveur TFTP	PE	4-18
delete	Supprime un fichier ou une image code	PE	4-21
dir	Affiche une liste des fichiers de la mémoire Flash	PE	4-22
whichboot	Affiche les fichiers amorcés	PE	4-23
boot system	Spécifie le fichier ou l'image utilisés pour démarrer le système	GC	4-23

4.3.2.1 copy

Cette commande vous permet de déplacer (charger/télécharger) une image code ou un fichier de configuration entre la mémoire Flash du commutateur et un serveur TFTP. Lorsque vous enregistrez le code système ou les paramètres de configuration dans un fichier sur un serveur TFTP, ce fichier peut ensuite être à nouveau téléchargé sur le commutateur afin de restaurer le fonctionnement du système. Le succès du transfert du fichier dépend de l'accessibilité du serveur TFTP et de la qualité de la connexion réseau.

Syntaxe

copy file {file | running-config | startup-config | tftp}
copy running-config {file | startup-config | tftp}
copy startup-config {file | running-config | tftp}
copy tftp {file | running-config | startup-config}
copy tftp https-certificate

- **file** : mot-clé permettant de copier vers/depuis un fichier.
- **running-config** : mot-clé permettant de copier vers/depuis la configuration courante.
- **startup-config** : configuration utilisée pour l'initialisation du système.
- **tftp** : mot-clé permettant de copier vers/depuis un serveur TFTP.
- **https-certificate** : option permettant de spécifier un certificat, une clé privée et un mot de passe provenant d'une autorité de certification reconnue.

Configuration par défaut

Aucune

Mode de commande

Privileged Exec

Utilisation de la commande

- Le système vous invite à saisir les données requises pour exécuter la commande de copie.
- Le nom du fichier de configuration de destination ne doit pas contenir de barres obliques (\ ou /), il ne doit pas commencer par un point (.) et il ne peut pas dépasser 127 caractères sur le serveur TFTP ou 32 caractères sur le commutateur. (Caractères valables : A-Z, a-z, 0-9, « . », « - » , « _ »)
- En raison de la taille limitée de la mémoire flash, le commutateur ne prend en charge que deux fichiers de code de fonctionnement.
- Le nombre maximal de fichiers de configuration définis par l'utilisateur dépend de la mémoire disponible.
- Vous pouvez utiliser « Factory_Default_Config.cfg » comme source pour effectuer une copie depuis le fichier de configuration contenant les valeurs par défaut, mais vous ne pouvez pas l'utiliser comme destination.
- Pour remplacer la configuration du démarrage, vous pouvez utiliser **startup-config** comme destination.
- Les codes Boot ROM et Loader ne peuvent être ni chargés ni téléchargés vers/depuis le serveur TFTP. Seul un ingénieur Sun Service peut modifier les codes Boot ROM ou Loader.
- Pour plus d'informations sur la spécification d'un certificat https, voir « Navigation dans l'interface du navigateur Web », page 3-3.

Exemple

L'exemple suivant montre comment charger les paramètres de configuration dans un fichier du serveur TFTP :

```
Console#copy file tftp
Choose file type:
 1. config:  2. opcode: <1-2>: 1
Source file name: startup
TFTP server ip address: 10.1.0.99
Destination file name: startup.01
TFTP completed.
Success.

Console#
```

L'exemple suivant montre comment copier la configuration courante dans un fichier :

```
Console#copy running-config file
destination file name : startup
Write to FLASH Programming.
\Write to FLASH finish.
Success.

Console#
```

L'exemple suivant montre comment télécharger un fichier de configuration :

```
Console#copy tftp startup-config
TFTP server ip address: 10.1.0.99
Source configuration file name: startup.01
Startup configuration file name [startup]:
Write to FLASH Programming.
\Write to FLASH finish.
Success.

Console#
```

L'exemple suivant montre comment enregistrer un certificat de sécurité relatif à un site sur un serveur TFTP. Le commutateur est ensuite réamorcé afin d'activer le certificat.

```
Console#copy tftp https-certificate

      TFTP server ip address: 10.1.0.19
      Source certificate file name: SS-certificate

      Source private file name: SS-private
      Private password: ********

Success.
Console#reload
System will be restarted, continue <y/n>? y
```

4.3.2.2 delete

Cette commande permet de supprimer un fichier ou une image.

Syntaxe

delete *filename*

filename : Nom du fichier de configuration ou de l'image.

Configuration par défaut

Aucune

Mode de commande

Privileged Exec

Utilisation de la commande

- Si le type de fichier est boot-ROM ou est utilisé pour le démarrage du système, le fichier ne peut pas être supprimé.
- « Factory_Default_Config.cfg » ne peut pas être supprimé.

Exemple

Cet exemple montre comment supprimer le fichier de configuration test2.cfg de la mémoire flash.

```
Console#delete test2.cfg
Console#
```

Commandes associées

dir (4-22)

4.3.2.3 dir

Cette commande permet d'afficher une liste des fichiers de la mémoire Flash.

Syntaxe

dir [boot-rom | **config** | **opcode [:***filename***]]**

Le type de fichier ou d'image à afficher comprend :

- **boot-rom** : ROM d'amorçage.
- **config** : Fichier de configuration.
- **opcode** : Nom du fichier ou de l'image. Si ce fichier existe mais contient des erreurs, les informations le concernant ne s'affichent pas.
- *filename* : Nom du fichier à afficher.

Configuration par défaut

Aucune

Mode de commande

Privileged Exec

Utilisation de la commande

- Si vous entrez la commande **dir** sans paramètres, le système affiche tous les fichiers.
- Les informations sur les fichiers sont présentées ci-dessous :

TABLEAU 4-1 Infos fichiers

Intitulé de colonne	Description
file name	Nom du fichier.
file type	Types de fichier : Boot-Rom, Operation Code et Config.
startup	Indique si ce fichier est utilisé au démarrage du système.
size	Longueur du fichier en octets.

Exemple

L'exemple suivant montre comment afficher toutes les informations concernant les fichiers :

```
Console#dir
                      file name      file type startup size (byte)
------------------------------ -------------- ------- -----------
                      diag_0060 Boot-Rom image       Y      111360
                      run_01642 Operation Code       N     1074304
                       run_0200 Operation Code       Y     1083008
     Factory_Default_Config.cfg    Config File       N        2574
                        startup    Config File       Y        2710
-----------------------------------------------------------------
                                      Total free space:         0
Console#
```

4.3.2.4 whichboot

Cette commande permet d'afficher les fichiers amorcés au démarrage du système.

Configuration par défaut

Aucune

Mode de commande

Privileged Exec

Utilisation de la commande

Voir TABLEAU 4-1, page 4-22 et suivantes pour une description des informations fichiers affichées par cette commande.

Exemple

L'exemple ci-dessous montre les informations affichées par la commande **whichboot**.

```
Console#whichboot
        file name      file type startup size (byte)
---------------- -------------- ------- -----------
        diag_0060 Boot-Rom image       Y      111360
         run_0200 Operation Code       Y     1083008
          startup    Config File       Y        2710
Console#
```

4.3.2.5 boot system

Cette commande permet de spécifier le fichier ou l'image utilisés pour démarrer le système.

Syntaxe

boot system {**boot-rom** | **config** | **opcode**}: *filename*

Le type de fichier ou d'image à définir comme valeur par défaut comprend :

- **boot-rom** : ROM d'amorçage.
- **config** : Fichier de configuration.
- **opcode** : Code de fonctionnement « run-time ».

Les deux points (:) sont requis.

filename : Nom du fichier de configuration ou de l'image

Configuration par défaut

Aucune

Mode de commande

Global Configuration

Utilisation de la commande

- Deux points (:) sont requis après le type de fichier spécifié.
- Si le fichier contient une erreur, il ne peut pas être défini comme fichier par défaut.

Exemple

```
Console(config)#boot system config: startup
Console(config)#
```

Commandes associées

dir (4-22)
whichboot (4-23)

4.3.3 Commandes de gestion du système

Ces commandes permettent de gérer les journaux système, les noms d'utilisateur, les options de configuration du navigateur ainsi que d'afficher ou de configurer plusieurs autres informations sur le système.

Commande	Fonction	Mode	Page
Commande de description du périphérique			
hostname	Spécifie ou modifie le nom d'hôte du périphérique.	GC	4-25
Commandes d'accès utilisateur			
username	Etablit un système d'authentification à la connexion basé sur le nom de l'utilisateur.	GC	4-26
enable password	Définit un mot de passe pour gérer l'accès au niveau Privileged Exec.	GC	4-27
Commandes du serveur Web			
ip http port	Spécifie le port que doit utiliser l'interface du navigateur Web.	GC	4-28
ip http server	Permet de contrôler ou configurer le commutateur depuis un navigateur.	GC	4-29
Commande des trames Jumbo			
jumbo-frame	Active la prise en charge des trames Jumbo.	GC	4-29
Commandes de journalisation des événements			
logging on	Contrôle la journalisation des messages d'erreur.	GC	4-30
logging history	Limite l'enregistrement des messages syslog dans la mémoire du commutateur sur la base de leur gravité.	GC	4-31

Commande	Fonction	Mode	Page
clear logging	Efface les messages du tampon de journalisation.	PE	4-32
show logging	Affiche l'état de la journalisation.	PE	4-33
Commandes de l'état du système			
show startup-config	Affiche le contenu du fichier de configuration (enregistré dans la mémoire Flash) utilisé pour démarrer le système.	PE	4-34
show running-config	Affiche les données de configuration actuellement utilisées.	PE	4-36
show system	Affiche les informations système.	NE, PE	4-38
show users	Affiche toutes les sessions actives de la console et de Telnet, comprenant le nom d'utilisateur, le délai d'inactivité et l'adresse IP des clients Telnet.	NE, PE	4-39
show version	Affiche des informations sur la version du système.	NE, PE	4-40

4.3.3.1 hostname

Cette commande permet de spécifier ou de modifier le nom d'hôte pour ce périphérique. Utilisez la forme **no** pour restaurer le nom d'hôte par défaut.

Syntaxe

hostname *name*
no hostname

name : Nom de cet hôte. (Longueur maximale : 255 caractères)

Configuration par défaut

Aucune

Mode de commande

Global Configuration

Exemple

```
Console(config)#hostname Server_Chassis_35
Console(config)#
```

4.3.3.2 username

Cette commande permet d'ajouter des utilisateurs nommés, de demander l'authentification à la connexion, de spécifier ou de modifier le mot de passe d'un utilisateur (ou de spécifier qu'aucun mot de passe n'est requis), ou encore de spécifier/modifier le niveau d'accès d'un utilisateur. Utilisez la forme **no** pour supprimer un nom d'utilisateur.

Syntaxe

username *name* {**access-level** *level* | **nopassword** | **password** {**0** | **7**} *password*}
no username *name*

- *name* : Nom de cet utilisateur.
  (Longueur maximale : 8 caractères ; nombre maximal d'utilisateurs : 5)
- **access-level** *level* : Spécifie le niveau de l'utilisateur.
  Le périphérique possède deux niveaux privilégiés prédéfinis :
  0: Normal Exec, **15**: Privileged Exec. (Les niveaux 1 à 14 ne sont pas utilisés.)
- **nopassword** : Aucun mot de passe n'est requis pour que cet utilisateur puisse se connecter.
- {**0** | **7**} : 0 signifie saisie d'un mot de passe simple, 7 signifie saisie d'un mot de passe chiffré.
- **password** *password* : Mot de passe permettant l'authentification de l'utilisateur.
  (Longueur maximale : 8 caractères de texte simple, 32 caractères chiffrés, respectant la casse)

Configuration par défaut

- Le niveau d'accès par défaut est Normal Exec.
- Les mots de passe par défaut sont « guest » en mode « Normal Exec » et « admin » en mode « Privileged Exec ».

  Les paramètres d'usine par défaut pour les noms d'utilisateur et les mots de passe sont les suivants :

TABLEAU 4-2 Noms d'utilisateur et mots de passe par défaut

Nom d'utilisateur	Niveau d'accès	Mot de passe
guest	0	guest
admin	15	admin

Mode de commande

Global Configuration

Utilisation de la commande

Il n'est pas nécessaire de spécifier des mots de passe chiffrés sur la ligne de commande. L'option 7 est utilisée en interne par le commutateur au démarrage du système afin de pouvoir lire les mots de passe chiffrés enregistrés dans le fichier de configuration.

Exemple

L'exemple suivant montre comment définir le niveau d'accès et le mot de passe pour un utilisateur.

```
Console(config)#username bob access-level 15
Console(config)#username bob password 0 smith
Console(config)#
```

4.3.3.3 enable password

Après vous être connecté au système pour la première fois, vous devez définir le mot de passe Privileged Exec. Conservez-le en lieu sûr. Cette commande vous permet de gérer l'accès au niveau Privileged Exec depuis le niveau Normal Exec. Utilisez la forme **no** pour réinitialiser le mot de passe par défaut.

Syntaxe

enable password [**level** *level*] {**0** | **7**} *password*
no enable password [**level** *level*]

- **level** *level* : Niveau **15** pour Privileged Exec. (Les niveaux 0 à 14 ne sont pas utilisés.)
- {**0** | **7**} : 0 signifie saisie d'un mot de passe simple, 7 signifie saisie d'un mot de passe chiffré.
- *password* : mot de passe pour ce niveau privilégié. (Longueur maximale : 8 caractères de texte simple, 32 caractères chiffrés, respectant la casse)

Configuration par défaut

- La valeur par défaut est 15.
- Le mot de passe par défaut est « super ».

Mode de commande

Global Configuration

Utilisation de la commande

- Vous ne pouvez pas définir un mot de passe nul. Vous devrez entrer un mot de passe pour passer du mode de commande « Normal Exec » à « Privileged Exec » à l'aide de la commande **enable** (page 4-13).
- Il n'est pas nécessaire de spécifier des mots de passe chiffrés sur la ligne de commande. L'option 7 est utilisée en interne par le commutateur au démarrage du système afin de pouvoir lire les mots de passe chiffrés enregistrés dans le fichier de configuration.

Exemple

```
Console(config)#enable password level 15 0 admin
Console(config)#
```

Commandes associées

enable (4-13)

4.3.3.4 ip http port

Cette commande permet de spécifier le numéro du port TCP utilisé par l'interface du navigateur Web. Utilisez la forme **no** pour utiliser le port par défaut.

Syntaxe

ip http port *port-number*
no ip http port

port-number : Port TCP que doit utiliser l'interface du navigateur. (Plage : 1-65535)

Configuration par défaut

80

Mode de commande

Global Configuration

Exemple

```
Console(config)#ip http port 769
Console(config)#
```

Commandes associées

ip http server (4-29)

4.3.3.5 ip http server

Cette commande permet d'autoriser le contrôle et la configuration de ce périphérique depuis un navigateur. Utilisez la forme **no** pour désactiver cette fonction.

Syntaxe

ip http server
no ip http server

Configuration par défaut

Activée

Mode de commande

Global Configuration

Exemple

```
Console(config)#ip http server
Console(config)#
```

Commandes associées

ip http port (4-28)

4.3.3.6 jumbo-frame

Cette commande permet d'activer la prise en charge des trames Jumbo. Utilisez la forme **no** pour désactiver cette fonction.

Syntaxe

jumbo-frame
no jumbo-frame

Configuration par défaut

Désactivée

Mode de commande

Global Configuration

Utilisation de la commande

- Le commutateur assure un meilleur débit pour les transferts de grands volumes de données séquentielles en prenant en charge les trames Jumbo jusqu'à 9 000 octets. Comparées aux trames Ethernet standard qui ne fonctionnent que jusqu'à 1,5 Ko, les trames Jumbo réduisent considérablement les ressources requises pour traiter les zones d'encapsulage du protocole pour chaque paquet.

- Pour pouvoir utiliser les trames Jumbo, les noeuds finaux source et destination (tels qu'un ordinateur ou un serveur) doivent prendre cette fonction en charge. Par ailleurs, lorsque la connexion fonctionne en duplex, tous les commutateurs du réseau entre les deux noeuds finaux doivent pouvoir accepter la plus grande taille des trames. Par ailleurs, dans le cas des connexions en « semi duplex », tous les périphériques du domaine de collision doivent prendre les trames Jumbo en charge.
- L'activation des trames Jumbo limite le seuil maximal du contrôle des orages de diffusion à 64 paquets par seconde. (Voir la commande **switchport broadcast** à la page 4-81.)

Exemple

```
Console(config)#jumbo-frame
Console(config)#
```

4.3.3.7 logging on

Cette commande permet de contrôler la journalisation des messages d'erreur. Elle envoie des messages de débogage ou d'erreur à la mémoire du commutateur. Utilisez la forme **no** pour désactiver le processus de journalisation.

Syntaxe

logging on
no logging on

Configuration par défaut

Aucune

Mode de commande

Global Configuration

Utilisation de la commande

Le processus de journalisation détermine les messages d'erreur enregistrés dans la mémoire du commutateur. La commande **logging history** permet de déterminer le type de messages d'erreur à enregistrer.

Exemple

```
Console(config)#logging on
Console(config)#
```

Commandes associées

logging history (4-31)
clear logging (4-32)

4.3.3.8 logging history

Cette commande permet de limiter les messages syslog enregistrés dans la mémoire du commutateur sur la base de leur gravité. La forme **no** permet de restaurer les valeurs initiales de la journalisation des messages syslog.

Syntaxe

logging history {**flash** | **ram**} *level*
no logging history {**flash** | **ram**}

- **flash** : historique des événements enregistrés dans la mémoire flash (à savoir la mémoire permanente).
- **ram** : historique des événements enregistrés dans la mémoire RAM (à savoir la mémoire « nettoyée » à la réinitialisation du système).
- *level* : 0-7 (Les messages enregistrés vont du niveau sélectionné au niveau 0.)

TABLEAU 4-3 Niveaux d'erreur

Argument de niveau	Niveau	Description
debugging	7	Messages de débogage
informational	6	Messages d'information uniquement
notifications	5	Condition normale mais importante, telle qu'un démarrage à froid (« cold start »)
warnings	4	Conditions d'avertissement (par exemple, résultat « false », résultat inattendu)
errors	3	Conditions d'erreur (p.ex., saisie non valable, valeur par défaut utilisée)
critical	2	Conditions critiques (p.ex., allocation de mémoire ou erreur de mémoire libre - ressources épuisées)
alerts	1	Action immédiate requise
emergencies	0	Système inutilisable

* Il n'existe aucun message d'erreur de niveau 0 ou 1 pour la version courante du microprogramme.

Configuration par défaut

Flash : errors (niveau 3-0)
RAM : warnings (niveau 7-0)

Mode de commande

Global Configuration

Utilisation de la commande

Le niveau de message spécifié pour la mémoire flash doit être une priorité supérieure (à savoir portant un chiffre inférieur) à celle spécifiée pour la RAM.

Exemple

```
Console(config)#logging history ram 0
Console(config)#
```

4.3.3.9 clear logging

Cette commande permet d'effacer les messages depuis le tampon de journalisation.

Syntaxe

clear logging [**flash** | **ram**]

- **flash** : historique des événements enregistrés dans la mémoire flash (à savoir la mémoire permanente).
- **ram** : historique des événements enregistrés dans la mémoire RAM (à savoir la mémoire « nettoyée » à la réinitialisation du système).

Configuration par défaut

Flash et RAM

Mode de commande

Privileged Exec

Exemple

```
Console#clear logging
Console#
```

Commandes associées

show logging (4-33)

4.3.3.10 show logging

Cette commande permet d'afficher la configuration courante de la journalisation, de même que tous les messages système et événement enregistrés dans la mémoire.

Syntaxe

show logging {**flash** | **ram**}

- **flash** : historique des événements enregistrés dans la mémoire flash (à savoir la mémoire permanente).
- **ram** : historique des événements enregistrés dans la mémoire RAM (à savoir la mémoire « nettoyée » à la réinitialisation du système).

Configuration par défaut

Aucune

Mode de commande

Privileged Exec

Utilisation de la commande

Cette commande affiche les informations suivantes :

- `Syslog logging` : activation éventuelle de la journalisation système via la commande **logging on**.
- `History logging in FLASH/RAM :` niveaux des messages publiés sur la base de la commande **logging history**.
- Tous les messages système et événement enregistrés dans la mémoire.

Exemple

L'exemple suivant montre que la journalisation système est active, le niveau des messages pour la mémoire flash est « errors » (à savoir le niveau par défaut 3 - 0), le niveau des messages pour la RAM est debug (à savoir le niveau par défaut 7 - 0). Par ailleurs, il présente un exemple d'erreur.

```
Console#show logging flash
Syslog logging: Enable
History logging in FLASH: level errors
[0] 0:0:5 1/1/1
   "PRI_MGR_InitDefault function fails."
   level: 3, module: 13, function: 0, and event no.: 0
Console#show logging ram
Syslog logging: Enable
History logging in RAM: level debugging
[0] 0:0:5 1/1/1
   "PRI_MGR_InitDefault function fails."
   level: 3, module: 13, function: 0, and event no.: 0
Console#
```

Commandes associées

logging on (4-30)
logging history (4-31)

4.3.3.11 show startup-config

Cette commande permet d'afficher le fichier de configuration enregistré dans une mémoire non volatile utilisée pour démarrer le système.

Configuration par défaut

Aucune

Mode de commande

Privileged Exec

Utilisation de la commande

- Cette commande, utilisée avec la commande **show running-config**, permet de comparer les informations de la mémoire courante aux informations stockées dans la mémoire non volatile.
- Cette commande affiche les paramètres des modes de commande clés. Chaque groupe de modes est séparé par des symboles « ! » et comprend la commande du mode de configuration ainsi que les commandes correspondantes. Cette commande affiche les informations suivantes :
  - description du système (nom de l'hôte, emplacement, informations de contact) ;
  - chaînes de communauté SNMP ;
  - utilisateurs (noms, niveaux d'accès et mots de passe chiffrés) ;
  - base de données VLAN (identificateur, nom et état du VLAN) ;
  - paramètres de configuration des VLAN pour chaque interface ;
  - adresse IP du VLAN de gestion ;
  - séquence d'authentification de l'utilisateur, avec l'adresse du serveur d'authentification distant et le port UDP ;
  - tout paramètre configuré pour le port console et Telnet.

Exemple

```
Console#show startup-config
building startup-config, please wait.....
!
hostname R&D 5
snmp-server location WC 9
snmp-server contact Charles
```

```
!
snmp-server community private rw
snmp-server community public ro
!
username admin access-level 15
username admin password 7 21232f297a57a5a743894a0e4a801fc3
username guest access-level 0
username guest password 7 084e0343a0486ff05530df6c705c8bb4
enable password level 15 7 1b3231655cebb7a1f783eddf27d254ca
!
vlan database
 vlan 1 name DefaultVlan media ethernet state active
 vlan 2 name MgtVlan media ethernet state active
!
!
spanning-tree mst-configuration
 name XSTP REGION 0
!
interface ethernet SNP0
 description Blade Slot 1
 flowcontrol
 switchport allowed vlan add 1 untagged
 switchport native vlan 1
 spanning-tree edge-port
 spanning-tree link-type auto
.
.
interface vlan 2
 ip address 0.0.0.0 255.0.0.0
!!
no bridge-ext gvrp!
!
authentication login local
tacacs-server host 0.0.0.0
tacacs-server port 0
!
line console
!
!
line vty
!
!
end
Console#
```

Commandes associées

show running-config (4-36)

4.3.3.12 show running-config

Cette commande permet d'afficher les informations de configuration actuellement utilisées.

Configuration par défaut

Aucune

Mode de commande

Privileged Exec

Utilisation de la commande

- Cette commande, utilisée avec la commande **show startup-config**, permet de comparer les informations de la mémoire courante aux informations stockées dans la mémoire non volatile.
- Cette commande affiche les paramètres des modes de commande clés. Chaque groupe de modes est séparé par des symboles « ! » et comprend la commande du mode de configuration ainsi que les commandes correspondantes. Cette commande affiche les informations suivantes :
  - description du système (nom de l'hôte, emplacement, informations de contact) ;
  - chaînes de communauté SNMP ;
  - utilisateurs (noms, niveaux d'accès et mots de passe chiffrés) ;
  - base de données VLAN (identificateur, nom et état du VLAN) ;
  - paramètres de configuration des VLAN pour chaque interface ;
  - adresse IP du VLAN de gestion ;
  - séquence d'authentification de l'utilisateur, avec l'adresse du serveur d'authentification distant et le port UDP ;
  - tout paramètre configuré pour le port console et Telnet.

Exemple

```
Console#show running-config
building running-config, please wait.....
!
hostname R&D 5
snmp-server location WC 9
snmp-server contact Charles
!
snmp-server community private rw
snmp-server community public ro
```

```
!
username admin access-level 15
username admin password 7 21232f297a57a5a743894a0e4a801fc3
username guest access-level 0
username guest password 7 084e0343a0486ff05530df6c705c8bb4
enable password level 15 7 1b3231655cebb7a1f783eddf27d254ca
!
vlan database
 vlan 1 name DefaultVlan media ethernet state active
 vlan 2 name MgtVlan media ethernet state active
!
!
!
spanning-tree mst-configuration
!
interface ethernet SNP0
 description Blade Slot 0
 flowcontrol
 switchport allowed vlan add 1 untagged
 switchport native vlan 1
 spanning-tree edge-port
 spanning-tree link-type auto
.
.
interface vlan 2
 ip address 0.0.0.0 255.0.0.0
!
!
no bridge-ext gvrp
!
!
authentication login local
tacacs-server host 0.0.0.0
tacacs-server port 0
!
line console
!
line vty
!
!
end
Console#
```

Commandes associées

show startup-config (4-34)

4.3.3.13 show system

Cette commande permet d'afficher les informations système.

Configuration par défaut

Aucune

Mode de commande

Normal Exec, Privileged Exec

Utilisation de la commande

- Pour une description des éléments affichés par cette commande, reportez-vous à « Affichage des informations relatives au système », page 3-8.
- Les résultats POST devraient tous afficher « PASS ». Si l'un des tests POST indique « FAIL », contactez votre distributeur pour obtenir de l'aide.

Exemple

```
Console#show system
System description: Sun Fire B1600
System OID string: 1.3.6.1.4.1.42.2.24.1
System information
 System Up time: 0 days, 0 hours, 55 minutes, and 54.91 seconds
 System Name            : [NONE]
 System Location        : [NONE]
 System Contact         : [NONE]
 MAC address            : 00-00-e8-00-00-01
 Web server             : enable
 Web server port        : 80
 Web secure server      : enable
 Web secure server port : 443
 POST result

--- Performing Power-On Self Tests (POST) ---
UART Loopback Test ..................... PASS
Timer Test ............................. PASS
DRAM Test .............................. PASS
I2C Initialization ..................... PASS
Runtime Image Check .................... PASS
PCI Device Check ....................... PASS
Switch Driver Initialization ........... PASS
------------------- DONE --------------------
Console#
```

4.3.3.14 show users

Cette commande affiche toutes les sessions Console et Telnet actives, avec les noms d'utilisateur, les délais d'inactivité et les adresses IP des clients Telnet.

Configuration par défaut

Aucune

Mode de commande

Normal Exec, Privileged Exec

Utilisation de la commande

La session utilisée pour exécuter cette commande est identifiée par un symbole « * » situé en regard du numéro d'index de la ligne (à savoir de la session).

Exemple

```
Console#show users
 Username accounts:
  Username Privilege
  -------- ---------
     admin        15
     guest         0

 Online users:
  Line        Username Idle time (h:m:s) Remote IP addr.
  ----------- -------- ----------------- ---------------
* 0   console    admin           0:00:00
  1     vty 0    admin           0:04:37      10.1.0.19

Console#
```

4.3.3.15 show version

Cette commande permet d'afficher les informations des versions matérielle et logicielle du système.

Configuration par défaut

Aucune

Mode de commande

Normal Exec, Privileged Exec

Utilisation de la commande

Reportez-vous à « Affichage des versions logicielles du commutateur », page 3-17 pour des informations détaillées concernant les éléments logiciels. La signification des éléments matériels est la suivante :

- **Serial Number** : Numéro de série de la carte mère.
- **Service Tag** : Non applicable pour ce commutateur.
- **Hardware Version** : Version matérielle de la carte mère.
- **Number of Ports** : Nombre de ports sur ce commutateur.
- **Main Power Status** : État de l'alimentation pour le commutateur.
- **Redundant Power Status** : Non applicable à ce commutateur.

Exemple

```
Console#show version
Unit1
 Serial number          :1
 Service tag            :
 Hardware version       :R0B
 Number of ports        :25
 Main power status      :up
 Redundant power status :not present
Agent(master)
 Unit id                :1
 Loader version         :0.0.6.5
 Boot rom version       :0.0.7.3
 Operation code version :1.0.0.1
Console#
```

4.3.4 Commandes d'authentification

Vous pouvez configurer ce commutateur pour authentifier les utilisateurs se connectant au système à des fins de gestion à l'aide des méthodes d'authentification RADIUS ou TACACS.

RADIUS et TACACS sont des protocoles d'authentification à la connexion utilisant un logiciel tournant sur un serveur central pour gérer l'accès aux périphériques réseau les prenant en charge. Un serveur d'authentification contient une base de données comprenant plusieurs paires nom d'utilisateur/mot de passe avec les niveaux de privilèges associés pour chaque utilisateur ou groupe requérant un accès au commutateur dans le but de gérer celui-ci.

Commande	Fonction	Mode	Page
Méthode d'authentification			
authentication login	Définit la méthode d'authentification à la connexion et sa priorité.	GC	4-42
Client RADIUS			
radius-server host	Spécifie le serveur RADIUS.	GC	4-43
radius-server port	Définit le port réseau du serveur RADIUS.	GC	4-43
radius-server key	Définit la clé de chiffrement RADIUS.	GC	4-44
radius-server retransmit	Définit le nombre de tentatives.	GC	4-44
radius-server timeout	Définit l'intervalle entre les envois de requêtes d'authentification.	GC	4-45
show radius-server	Affiche les paramètres RADIUS courants.	PE	4-45
Client TACACS			
tacacs-server host	Spécifie le serveur TACACS.	GC	4-46
tacacs-server port	Définit le port réseau du serveur TACACS.	GC	4-46
tacacs-server key	Définit la clé de chiffrement TACACS.	GC	4-47
show tacacs-server	Affiche les paramètres TACACS courants.	PE	4-47

4.3.4.1 authentication login

Cette commande permet de définir la méthode d'authentification à la connexion et sa priorité. Utilisez la forme **no** pour restaurer la valeur par défaut.

Syntaxe

authentication login {[**local**] [**radius**] [**tacacs**]}
no authentication login

- **local** : Utilisez le mot de passe local.
- **radius** : Utilisez le mot de passe du serveur RADIUS.
- **tacacs** : Utilisez le mot de passe du serveur TACACS.

Les méthodes d'authentification peuvent être spécifiées dans un ordre quelconque.

Configuration par défaut

Aucune

Mode de commande

Global Configuration

Utilisation de la commande

- RADIUS utilise UDP alors que TACACS utilise TCP. UDP n'offre qu'une livraison « best effort » (sans garantie) alors que TCP propose un transfert orienté sur la connexion. De même, remarquez que RADIUS ne chiffre le mot de passe que dans le paquet de requête d'accès du client au serveur, alors que TACACS chiffre l'ensemble du paquet.
- L'authentification à la connexion par RADIUS et TACACS peut contrôler les droits de gestion par le biais du port console, du navigateur Web ou de Telnet. Ces options d'accès doivent être configurées sur le serveur d'authentification.
- L'authentification à la connexion par RADIUS et TACACS affecte un niveau de privilèges spécifique à chaque paire nom d'utilisateur/mot de passe. Le nom d'utilisateur, le mot de passe et le niveau de privilèges doivent être configurés sur le serveur d'authentification.
- Vous pouvez spécifier deux ou trois méthodes d'authentification dans une seule commande afin d'indiquer la séquence d'authentification. Par exemple, si vous entrez « **authentification login radius local** », le nom d'utilisateur et le mot de passe sur le serveur RADIUS sont vérifiés en premier lieu. Si le serveur RADIUS n'est pas disponible, le nom d'utilisateur et le mot de passe locaux sont vérifiés.

Exemple

```
Console(config)#authentication login radius
Console(config)#
```

Commandes associées

username : pour la définition du nom de l'utilisateur local et du mot de passe (4-26)

4.3.4.2 radius-server host

Cette commande permet de spécifier le serveur RADIUS. Utilisez la forme **no** pour restaurer la valeur par défaut.

Syntaxe

radius-server host *host_ip_address*
no radius-server host

host_ip_address : Adresse IP du serveur.

Configuration par défaut

10.11.12.13

Mode de commande

Global Configuration

Exemple

```
Console(config)#radius-server host 192.168.1.25
Console(config)#
```

4.3.4.3 radius-server port

Cette commande permet de définir le port réseau du serveur RADIUS. Utilisez la forme **no** pour restaurer la valeur par défaut.

Syntaxe

radius-server port *port_number*
no radius-server port

port_number : port UDP du serveur RADIUS utilisé pour les messages d'authentification. (Plage : 1-65535)

Configuration par défaut

1812

Mode de commande

Global Configuration

Exemple

```
Console(config)#radius-server port 181
Console(config)#
```

4.3.4.4 radius-server key

Cette commande permet de définir la clé de chiffrement RADIUS. Utilisez la forme **no** pour restaurer la valeur par défaut.

Syntaxe

radius-server key *key_string*
no radius-server key

key_string : Clé de chiffrement utilisée pour authentifier l'accès du client à la connexion. Ne laissez pas d'espaces blancs dans la chaîne. (Longueur maximale : 20 caractères)

Configuration par défaut

Aucune

Mode de commande

Global Configuration

Exemple

```
Console(config)#radius-server key green
Console(config)#
```

4.3.4.5 radius-server retransmit

Cette commande permet de définir le nombre de tentatives. Utilisez la forme **no** pour restaurer la valeur par défaut.

Syntaxe

radius-server retransmit *number_of_retries*
no radius-server retransmit

number_of_retries : Nombre de tentatives effectuées par le commutateur pour authentifier les droits de connexion via le serveur RADIUS. (Plage : 1-30)

Configuration par défaut

2

Mode de commande

Global Configuration

Exemple

```
Console(config)#radius-server retransmit 5
Console(config)#
```

4.3.4.6 radius-server timeout

Cette commande permet de définir l'intervalle entre les demandes d'authentification transmises au serveur RADIUS. Utilisez la forme **no** pour restaurer la valeur par défaut.

Syntaxe

radius-server timeout *number_of_seconds*
no radius-server timeout

number_of_seconds : Nombre de secondes pendant lequel le commutateur attend une réponse avant de renvoyer une requête. (Plage : 1-65535)

Configuration par défaut

5

Mode de commande

Global Configuration

Exemple

```
Console(config)#radius-server timeout 10
Console(config)#
```

4.3.4.7 show radius-server

Cette commande permet d'afficher les paramètres courants du serveur RADIUS.

Configuration par défaut

Aucune

Mode de commande

Privileged Exec

Exemple

```
Console#show radius-server
Remote radius server configuration:
 Server IP address: 10.11.12.13
 Communication key with radius server: green
 Server port number: 1812
 Retransmit times: 2
 Request timeout: 5
Console#
```

4.3.4.8 tacacs-server host

Cette commande permet de spécifier le serveur TACACS. Utilisez la forme **no** pour restaurer la valeur par défaut.

Syntaxe

tacacs-server host *host_ip_address*
no tacacs-server host

host_ip_address : Adresse IP du serveur.

Configuration par défaut

Aucune

Mode de commande

Global Configuration

Exemple

```
Console(config)#tacacs-server host 192.168.1.25
Console(config)#
```

4.3.4.9 tacacs-server port

Cette commande permet de définir le port réseau du serveur TACACS. Utilisez la forme **no** pour restaurer la valeur par défaut.

Syntaxe

tacacs-server port *port_number*
no tacacs-server port

port_number : port UDP du serveur TACACS utilisé pour les messages d'authentification. (Plage : 1-65535)

Configuration par défaut

Aucune

Mode de commande

Global Configuration

Exemple

```
Console(config)#tacacs-server port 181
Console(config)#
```

4.3.4.10 tacacs-server key

Cette commande permet de définir la clé de chiffrement TACACS. Utilisez la forme **no** pour restaurer la valeur par défaut.

Syntaxe

tacacs-server key *key_string*
no tacacs-server key

key_string : Clé de chiffrement utilisée pour authentifier l'accès du client à la connexion. Ne laissez pas d'espaces blancs dans la chaîne. (Longueur maximale : 20 caractères)

Configuration par défaut

Aucune

Mode de commande

Global Configuration

Exemple

```
Console(config)#tacacs-server key green
Console(config)#
```

4.3.4.11 show radius-server

Cette commande permet d'afficher les paramètres courants du serveur TACACS.

Configuration par défaut

Aucune

Mode de commande

Privileged Exec

Exemple

```
Console#show tacacs-server
Remote TACACS server configuration:
 Server IP address: 10.11.12.13
 Communication key with tacacs server: green
 Server port number: 1824
Console#
```

4.3.5 Commandes SNMP

Ces commandes permettent de gérer l'accès au commutateur depuis les stations de gestion SNMP ainsi que les types d'erreur envoyés aux gestionnaires d'interruptions.

Commande	Fonction	Mode	Page
snmp-server community	Définit la chaîne de communauté permettant l'accès aux commandes SNMP	GC	4-48
snmp-server contact	Définit la chaîne de contact système	GC	4-49
snmp-server location	Définit la chaîne d'emplacement système	GC	4-50
snmp-server host	Spécifie le destinataire d'une opération de notification SNMP	GC	4-50
snmp-server enable traps	Permet au périphérique d'envoyer des interruptions SNMP ou des requêtes d'information (notifications SNMP)	GC	4-51
show snmp	Affiche l'état des communications SNMP	NE, PE	4-52

4.3.5.1 snmp-server community

Cette commande permet de définir la chaîne de communauté pour le protocole SNMP (Simple Network Management Protocol). Utilisez la forme **no** pour supprimer la chaîne spécifiée.

Syntaxe

snmp-server community *string* [**ro** | **rw**]
no snmp-server community *string*

- *string* : Chaîne de communauté agissant comme un mot de passe et autorisant l'accès au protocole SNMP. (Longueur maximale : 32 caractères, respectant la casse ; nombre maximal de chaînes : 5)
- **ro** : Spécifie l'accès en lecture seule. Les stations de gestion autorisées peuvent uniquement récupérer les objets MIB.
- **rw** : Spécifie l'accès en lecture/écriture. Les stations de gestion autorisées peuvent récupérer et modifier les objets MIB.

Configuration par défaut

- public - avec accès en lecture seule.
- private - avec accès en lecture/écriture.

Mode de commande

Global Configuration

Utilisation de la commande

La première commande **snmp-server community** entrée active toutes les versions de SNMP (SNMPv1 et SNMPv2c). La commande **no snmp-server community** désactive toutes les versions de SNMP.

Exemple

```
Console(config)#snmp-server community alpha rw
Console(config)#
```

4.3.5.2 snmp-server contact

Cette commande permet de définir la chaîne de contact du système. Utilisez la forme **no** pour supprimer les informations de contact du système.

Syntaxe

snmp-server contact *string*
no snmp-server contact

string : Chaîne décrivant les informations de contact du système. (Longueur maximale : 255 caractères)

Configuration par défaut

Aucune

Mode de commande

Global Configuration

Exemple

```
Console(config)#snmp-server contact Paul
Console(config)#
```

Commandes associées

snmp-server location (4-50)

4.3.5.3 snmp-server location

Cette commande permet de définir la chaîne d'emplacement système. Utilisez la forme **no** pour supprimer la chaîne d'emplacement.

Syntaxe

snmp-server location *text*
no snmp-server location

text : Chaîne décrivant l'emplacement du système. (Longueur maximale : 255 caractères)

Configuration par défaut

Aucune

Mode de commande

Global Configuration

Exemple

```
Console(config)#snmp-server location WC-19
Console(config)#
```

Commandes associées

snmp-server contact (4-49)

4.3.5.4 snmp-server host

Cette commande permet de spécifier le destinataire d'une opération de notification SNMP (Simple Network Management Protocol). Utilisez la forme **no** pour supprimer l'hôte spécifié.

Syntaxe

snmp-server host *host-addr community-string* **version** *version-number*
no snmp-server host *host-addr*

- *host-addr* : Nom ou adresse Internet de l'hôte (destinataire cible). (Adresses maximales de l'hôte : 5 adresses IP de destination pour les interruptions)
- *community-string* : Chaîne de communauté ressemblant à un mot de passe et envoyée avec l'opération de notification. Bien que vous puissiez définir cette chaîne à l'aide de la commande **snmp-server host** seule, nous vous recommandons de le faire en utilisant la commande **snmp-server community** avant la commande **snmp-server host**. (Longueur maximale : 32 caractères)
- *version-number* - {**1** | **2c**}
  Indique si l'hôte tourne sous SNMP version 1 ou version 2c.

Configuration par défaut

Aucune

Mode de commande

Global Configuration

Utilisation de la commande

Si vous n'entrez pas de commande **snmp-server host**, aucune notification n'est envoyée. Pour pouvoir configurer le commutateur afin qu'il envoie des notifications SNMP, vous devez entrer au moins une commande **snmp-server host**. Pour activer plusieurs hôtes, vous pouvez émettre une commande **snmp-server host** distincte pour chaque hôte.

La commande **snmp-server host** est utilisée en conjonction avec la commande **snmp-server enable traps**. Utilisez la commande **snmp-server enable traps** pour spécifier quelles notifications SNMP sont envoyées globalement. Pour qu'un hôte reçoive des notifications, vous devez entrer au moins une commande **snmp-server enable traps** et la commande **snmp-server host** pour celui-ci.

Toutefois, certains types de notification ne peuvent pas être contrôlés à l'aide de la commande **snmp-server enable traps**. Par exemple, certains types de notification sont toujours activés.

Exemple

```
Console(config)#snmp-server host 10.1.19.23 batman version 1
Console(config)#
```

Commandes associées

snmp-server enable traps (4-51)

4.3.5.5 snmp-server enable traps

Cette commande permet d'activer ce périphérique pour qu'il envoie des interruptions SNMP (Simple Network Management Protocol) ou des informations (notifications SNMP). Utilisez la forme **no** pour désactiver les notifications SNMP.

Syntaxe

snmp-server enable traps [**authentication** | **link-up-down**]
no snmp-server enable traps [**authentication** | **link-up-down**]

- **authentication** : Mot-clé permettant d'émettre des interruptions en cas d'échec de l'authentification.
- **link-up-down** : Mot-clé permettant d'émettre des interruptions à liaison ascendante ou descendante.

Configuration par défaut

Émet des interruptions d'authentification et des interruptions à liaison ascendante/descendante.

Mode de commande

Global Configuration

Utilisation de la commande

Si vous n'entrez pas de commande **snmp-server enable traps**, aucune notification contrôlée par cette commande n'est envoyée. Pour pouvoir configurer ce commutateur afin qu'il envoie des notifications SNMP, vous devez entrer au moins une commande **snmp-server enable traps**. Si vous entrez la commande sans mot-clé, les notifications d'authentification et les notifications à liaison ascendante/descendante sont activées. Si vous entrez la commande avec un mot-clé, seul le type de notification lié à ce mot-clé est activé.

La commande **snmp-server enable traps** est utilisée en conjonction avec la commande **snmp-server host**. Utilisez la commande **snmp-server host** pour spécifier quel(s) hôte(s) reçoi(ven)t des notifications SNMP. Pour envoyer des notifications, vous devez configurer au moins une commande **snmp-server host**.

Exemple

```
Console(config)#snmp-server enable traps link-up-down
Console(config)#
```

Commandes associées

snmp-server host (4-50)

4.3.5.6 show snmp

Cette commande permet de contrôler l'état des communications SNMP.

Configuration par défaut

Aucune

Mode de commande

Normal Exec, Privileged Exec

Utilisation de la commande

Cette commande fournit des informations sur les chaînes de communauté ainsi que sur les compteurs des unités de données des protocoles SNMP d'entrée et de sortie, et indique si la connexion SNMP a été activée avec la commande **snmp-server enable traps**.

Exemple

```
Console#show snmp

SNMP traps:
 Authentication: enable
   Link-up-down: enable

SNMP communities:
   1. private, and the privilege is read/write
   2. public, and the privilege is read-only

0 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    0 Get-next PDUs
    0 Set-request PDUs
0 SNMP packets output
    0 Too big errors
    0 No such name errors
    0 Bad values errors
    0 General errors
    0 Response PDUs
    0 Trap PDUs

SNMP logging: disabled
Console#
```

4.3.6 Commandes de ligne

Vous pouvez accéder au programme de configuration intégré en raccordant un périphérique compatible VT100 au port série du serveur. Ces commandes permettent de définir des paramètres de communication pour le port série ou Telnet (un terminal virtuel).

Remarque - Les paramètres de connexion pour l'interface série sont fixés à 8 bits de données, 1 bit d'arrêt, aucune parité et 9600 bps.

Commande	Fonction	Mode	Page
line	Identifie une ligne spécifique pour la configuration et démarre le mode de configuration de la ligne	GC	4-55
login	Active la vérification du mot de passe à la connexion	LC	4-56
password	Spécifie un mot de passe sur une ligne	LC	4-57
exec-timeout	Définit le délai attendu par l'interpréteur de commandes avant la détection d'une saisie utilisateur	LC	4-58
password-thresh	Définit le seuil d'intrusion du mot de passe, limitant ainsi le nombre de tentatives de connexion conclues par un échec	LC	4-59
silent-time*	Définit le délai pendant lequel la console de gestion reste inaccessible lorsque le nombre de tentatives de connexion infructueuses dépasse le seuil défini par la commande **password-thresh**	LC	4-60
show line	Affiche les paramètres d'une ligne de terminal	NE, PE	4-61

* Cette commande ne s'applique qu'au port série.

4.3.6.1 line

Cette commande permet d'identifier une ligne spécifique pour la configuration et de traiter les commandes de configuration de ligne suivantes.

Syntaxe

line {**console** | **vty**}

- **console** : Ligne de terminal console.
- **vty** : Terminal virtuel pour l'accès distant à la console (Telnet).

Configuration par défaut

Il n'y a aucune ligne par défaut.

Mode de commande

Global Configuration

Utilisation de la commande

Telnet est considéré comme une connexion terminal virtuelle et s'affiche sous la forme « Vty » dans les écrans tels que **show users**.

Exemple

Pour passer en mode de ligne console, entrez la commande suivante :

```
Console(config)#line console
Console(config-line)#
```

Commandes associées

show line (4-61)
show users (4-39)

4.3.6.2 login

Cette commande permet d'activer la vérification du mot de passe à la connexion. Utilisez la forme **no** pour désactiver la vérification du mot de passe et autoriser des connexions sans mot de passe.

Syntaxe

login [local]
no login

local : Sélectionnez la vérification du mot de passe local. L'authentification repose sur le nom d'utilisateur spécifié à l'aide de la commande **username**.

Configuration par défaut

login local

Mode de commande

Line Configuration

Utilisation de la commande

- Vous avez le choix entre trois modes d'authentification proposés par le commutateur lui-même à la connexion :
  - **login** sélectionne l'authentification par un seul mot de passe global tel que spécifié par la commande de configuration de ligne **password**. Lorsque vous utilisez cette méthode, l'interface de gestion démarre en mode « Normal Exec (NE) ».
  - **login local** sélectionne l'authentification par le nom d'utilisateur et le mot de passe tels que spécifiés par la commande **username** (paramètre par défaut). Lorsque vous utilisez cette méthode, l'interface de gestion démarre en mode « Normal Exec (NE) » ou « Privileged Exec (PE) », selon le niveau d'accès de l'utilisateur (0 ou 15, respectivement).
  - **no login** ne sélectionne aucune authentification. Lorsque vous utilisez cette méthode, l'interface de gestion démarre en mode « Normal Exec (NE) ».
- Cette commande gère l'authentification à la connexion par le biais du commutateur lui-même. Pour configurer les noms d'utilisateur et les mots de passe pour les serveurs d'authentification distants, vous devez utiliser le logiciel RADIUS ou TACACS installé sur ces serveurs.

Exemple

```
Console(config-line)#login local
Console(config-line)#
```

Commandes associées

username (4-26)
password (4-57)

4.3.6.3 password

Cette commande permet de spécifier le mot de passe pour une ligne. Utilisez la forme **no** pour supprimer le mot de passe.

Syntaxe

password {**0** | **7**} *password*
no password

- {**0** | **7**} - 0 signifie saisie d'un mot de passe simple, 7 signifie saisie d'un mot de passe chiffré.
- *password* : Chaîne de caractères qui spécifie le mot de passe de ligne. (Longueur maximale : 8 caractères de texte simple, 32 caractères chiffrés, respectant la casse)

Configuration par défaut

Aucun mot de passe n'est affecté.

Mode de commande

Line Configuration

Utilisation de la commande

- Lorsqu'une connexion est démarrée sur une ligne avec une protection par mot de passe, le système vous invite à saisir le mot de passe. Si vous entrez le bon mot de passe, le système affiche une invite. Vous pouvez utiliser la commande **password-thresh** pour définir le nombre de fois qu'un utilisateur peut entrer un mot de passe incorrect avant que le système interrompe la connexion et renvoie le terminal à l'état inactif.
- Il n'est pas nécessaire de spécifier des mots de passe chiffrés sur la ligne de commande. L'option 7 est utilisée en interne par le commutateur au démarrage du système afin de pouvoir lire les mots de passe chiffrés enregistrés dans le fichier de configuration.

Exemple

```
Console(config-line)#password 0 secret
Console(config-line)#
```

Commandes associées

login (4-56)
password-thresh (4-59)

4.3.6.4 exec-timeout

Cette commande vous permet de définir le délai pendant lequel le système attend la saisie utilisateur avant de mettre un terme à la session courante. Utilisez la forme **no** pour restaurer la valeur par défaut.

Syntaxe

exec-timeout [*seconds*]
no exec-timeout

seconds : Nombre entier spécifiant le nombre de secondes.
(Plage : 0 - 65535 secondes ; 0 : no timeout)

Configuration par défaut

ILC : No timeout
Telnet : 10 minutes

Mode de commande

Line Configuration

Utilisation de la commande

- Si une saisie utilisateur est détectée pendant l'intervalle de temporisation, la session reste ouverte ; dans le cas contraire, la session est terminée.
- Cette commande s'applique aux connexions console série et Telnet (mais vous ne pouvez pas désactiver la temporisation pour Telnet).

Exemple

Pour définir la temporisation à deux minutes, entrez cette commande :

```
Console(config-line)#exec-timeout 120
Console(config-line)#
```

4.3.6.5 password-thresh

Cette commande permet de définir le seuil d'intrusion du mot de passe qui limite le nombre de tentatives de connexion infructueuses. Utilisez la forme **no** pour supprimer la valeur du seuil.

Syntaxe

password-thresh *threshold*
no password-thresh

threshold : Nombre de tentatives de saisie de mot de passe autorisées. (Plage : 1-120; 0: no threshold)

Configuration par défaut

La valeur par défaut est trois tentatives.

Mode de commande

Line Configuration

Utilisation de la commande

- Lorsque le seuil des tentatives de connexion est atteint sur le port console, l'interface du système reste inaccessible pendant un délai spécifié avant d'autoriser la tentative de connexion suivante. (Utilisez la commande **silent-time** pour définir cet intervalle.) Lorsque ce seuil est atteint pour Telnet, l'interface de connexion Telnet se ferme.
- Cette commande s'applique tant aux connexions de la console locale qu'aux connexions Telnet.

Exemple

Pour définir le seuil du mot de passe à cinq tentatives, entrez cette commande :

```
Console(config-line)#password-thresh 5
Console(config-line)#
```

Commandes associées

silent-time (4-60)

4.3.6.6 silent-time

Cette commande permet de définir le délai pendant laquelle la console de gestion est inaccessible lorsque le nombre de tentatives de connexion infructueuses dépasse le seuil défini par la commande **password-thresh**. Utilisez la forme **no** pour supprimer la valeur du délai d'inaccessibilité.

Syntaxe

silent-time [*seconds*]
no silent-time

seconds : Nombre de secondes pendant lequel la console doit rester inaccessible. (Plage : 0-65535 ; 0 : no silent-time)

Configuration par défaut

La valeur par défaut est no silent-time.

Mode de commande

Line Configuration

Exemple

Pour définir le délai d'inaccessibilité à 60 secondes, entrez cette commande :

```
Console(config-line)#silent-time 60
Console(config-line)#
```

Commandes associées

password-thresh (4-59)

4.3.6.7 show line

Cette commande permet d'afficher les paramètres de la ligne de terminal.

Syntaxe

show line [console | vty]

- **console** : Ligne de terminal console.
- **vty** : Terminal virtuel pour l'accès distant à la console (Telnet).

Configuration par défaut

Affiche toutes les lignes

Mode de commande

Normal Exec, Privileged Exec

Exemple

Pour afficher les paramètres de connexion de toutes les lignes, entrez cette commande :

```
Console#show line
 Console configuration:
  Password threshold: 3 times
  Interactive timeout: Disabled
  Silent time: Disabled
  Baudrate: 9600
  Databits: 8
  Parity: none
  Stopbits: 1

Vty configuration:
  Password threshold: 3 times
  Interactive timeout: 600
Console#
```

4.3.7 Commandes IP

Par défaut, le commutateur recherche son adresse IP, sa passerelle par défaut et son masque de sous-réseau à l'aide de DHCP.

Vous pouvez configurer manuellement une adresse IP spécifique ou ordonner au périphérique d'obtenir une adresse par le biais d'un serveur DHCP ou BOOTP. Les adresses IP valables se composent de quatre nombres décimaux, de 0 à 255, séparés par des points. Aucun autre format n'est accepté par le logiciel.

Commande	Fonction	Mode	Page
Configuration IP			
ip address	Définit l'adresse IP de ce périphérique	IC	4-62
ip dhcp restart	Soumet une requête client BOOTP ou DCHP	PE	4-64
ip dhcp client-identifier	Spécifie l'identificateur du client DHCP pour le commutateur. Remarquez que le contrôleur système affecte l'identificateur du client pour le commutateur à chaque démarrage de celui-ci. C'est pourquoi nous vous déconseillons de spécifier un identificateur de client.	VC	4-64
ip default-gateway	Définit la passerelle par défaut par le biais de laquelle une station de gestion intrabande peut atteindre ce périphérique	GC	4-65
show ip interface	Affiche les paramètres IP de ce périphérique	PE	4-66
show ip redirects	Affiche la passerelle par défaut configurée pour ce périphérique	PE	4-67
ping	Envoie des paquets de requêtes d'écho ICMP à un autre noeud du réseau	NE, PE	4-67
Filtrage des paquets IP			
ip filter	Empêche des paquets IP spécifiques d'entrer sur le port de gestion interne (NETMGT) depuis les autres ports du commutateur	GC	4-68
show ip filter	Affiche les règles de filtrage ou les paquets capturés	PE	4-72

4.3.7.1 ip address

Cette commande permet de définir l'adresse IP du périphérique. Utilisez la forme **no** pour restaurer l'adresse IP par défaut.

Syntaxe

ip address {*ip-address netmask* | **bootp** | **dhcp**}
no ip address

- *ip-address* : Adresse IP
- *netmask* : Masque du sous-réseau IP associé. Ce masque identifie l'adresse de l'hôte utilisée pour le routage vers des sous-réseaux spécifiques.
- **bootp** : Obtient l'adresse IP depuis BOOTP.
- **dhcp** : Obtient l'adresse IP depuis DHCP.

Configuration par défaut

Le paramètre par défaut est : dhcp

Mode de commande

Configuration de l'interface (VLAN)

Utilisation de la commande

- Vous pouvez configurer manuellement une adresse IP spécifique ou ordonner au périphérique d'obtenir une adresse par le biais d'un serveur DHCP ou BOOTP. La valeur usine par défaut est DHCP. Pour être valable, une adresse IP doit se composer de quatre nombres, de 0 à 255, séparés par des points. Aucun autre format n'est accepté par le programme de configuration.
- Si vous sélectionnez l'option **bootp** ou **dhcp**, IP est activé, mais ne fonctionne pas avant qu'une réponse BOOTP ou DHCP ait été reçue. Des requêtes sont diffusées périodiquement par ce périphérique dans un effort visant à apprendre son adresse IP. (Les valeurs DHCP/BOOTP peuvent inclure l'adresse IP, le masque de sous-réseau et la passerelle par défaut.)
- Vous pouvez démarrer la diffusion de requêtes BOOTP ou DHCP en entrant la commande **ip dhcp restart** ou en réinitialisant le commutateur.

Remarque - L'adresse IP du commutateur est en fait l'adresse IP du VLAN contenant le port de gestion (NETMGT). Par défaut, le port de gestion se trouve sur le VLAN 2. Par conséquent, c'est en affectant une adresse IP au VLAN 2 que vous configurez un accès réseau au commutateur. Seul le VLAN contenant le port de gestion doit se voir affecter une adresse IP. Lorsque vous affectez une adresse IP à un VLAN quelconque, l'adresse IP originale est immédiatement désactivée, et la nouvelle adresse prend effet simultanément.

Exemple

Dans l'exemple suivant, une adresse est affectée au périphérique dans le VLAN 2.

```
Console(config)#interface vlan 2
Console(config-if)#ip address 192.168.1.5 255.255.255.0
Console(config-if)#
```

Commandes associées

ip dhcp restart (4-64)

4.3.7.2 ip dhcp restart

Cette commande permet d'initier une requête client BOOTP ou DCHP.

Configuration par défaut

Aucune

Mode de commande

Privileged Exec

Utilisation de la commande

- Le DHCP requiert que le serveur réaffecte la dernière adresse du client si elle est disponible.
- Si le serveur BOOTP ou DHCP a été déplacé vers un autre domaine, la portion réseau de l'adresse fournie au client sera basée sur ce nouveau domaine.

Exemple

Dans l'exemple suivant, la même adresse est réaffectée au périphérique.

```
Console(config)#interface vlan 2
Console(config-if)#ip address dhcp
Console(config-if)#exit
Console#ip dhcp restart
Console#show ip interface
IP interface vlan
 IP address and netmask: 10.1.0.54 255.255.255.0 on VLAN 2,
 and address mode: DHCP.
Console#
```

Commandes associées

ip address (4-62)

4.3.7.3 ip dhcp client-identifier

Cette commande permet de spécifier l'identificateur du client DHCP pour ce commutateur. Utilisez la forme **no** pour supprimer cet identificateur.

Remarque - L'identificateur du client est écrasé par le contrôleur système lors du réamorçage suivant du système ou du commutateur. La commande client-identifier sera supprimée de la prochaine version du microprogramme.

Syntaxe

ip dhcp client-identifier {**text** *text* | **hex** *hex*}
no ip dhcp client-identifier

- *text* : Chaîne de texte. (Plage : 1-15 caractères)
- *hex* : Valeur hexadécimale.

Configuration par défaut

L'identificateur du client DHCP est fournie par le contrôleur système du module SSC lorsque le contrôleur système réinitialise le commutateur. C'est la raison pour laquelle nous vous déconseillons de modifier cette valeur depuis l'interface de ligne de commande du commutateur. Pour plus d'informations sur l'identificateur du client DHCP pour le commutateur et les autres composants du châssis, reportez-vous au *Manuel d'installation du logiciel du châssis Sun Fire™ B1600 pour serveurs Blade*.

Mode de commande

Interface Configuration (VLAN)

Utilisation de la commande

- Cette commande permet d'inclure un identificateur client dans toutes les communications établies avec le serveur DHCP. Le type de données utilisé dépend des exigences de votre serveur DHCP.
- L'identificateur du client spécifié dans cette commande est écrasé par le contrôleur système lors de son réamorçage suivant.

Exemple

```
Console(config)#interface vlan 2
Console(config-if)#ip dhcp client-identifier hex 00-00-e8-66-65-72
Console(config-if)#
```

Commandes associées

ip dhcp restart (4-64)

4.3.7.4 ip default-gateway

Cette commande permet d'établir une route statique entre ce périphérique et les stations de gestion existant sur un autre segment du réseau. Utilisez la forme **no** pour supprimer la route statique.

Syntaxe

ip default-gateway *gateway*
no ip default-gateway

gateway : Adresse IP de la passerelle par défaut.

Configuration par défaut

Aucune route statique n'est définie.

Mode de commande

Global Configuration

Utilisation de la commande

Une passerelle doit être définie si la station de gestion se trouve dans un segment UP différent.

Exemple

L'exemple suivant définit une passerelle par défaut pour ce périphérique :

```
Console(config)#ip default-gateway 10.1.0.254
Console(config)#
```

Commandes associées

show ip redirects (4-67)

4.3.7.5 show ip interface

Cette commande permet d'afficher les paramètres d'une interface IP.

Configuration par défaut

Toutes les interfaces

Mode de commande

Privileged Exec

Utilisation de la commande

Ce commutateur ne peut recevoir qu'une seule adresse IP. Celle-ci est utilisée pour la gestion du commutateur.

Exemple

```
Console#show ip interface
 IP address and netmask: 10.1.0.54 255.255.255.0 on VLAN 2,
 and address mode: User specified.
Console#
```

Commandes associées

show ip redirects (4-67)

4.3.7.6 show ip redirects

Cette commande permet d'afficher la passerelle par défaut configurée pour ce périphérique.

Configuration par défaut

Aucune

Mode de commande

Privileged Exec

Exemple

```
Console#show ip redirects
ip default gateway 10.1.0.254
Console#
```

Commandes associées

ip default-gateway (4-65)

4.3.7.7 ping

Cette commande permet d'envoyer des paquets de requêtes d'échos ICMP à un autre noeud du réseau.

Syntaxe

ping *host* [**count** *count*][**size** *size*]

- *host* : Adresse IP de l'hôte.
- *count* : Nombre de paquets à envoyer. (Plage : 1-16 ; Par défaut : 5)
- *size* : Nombre d'octets dans un paquet. (Plage : 32-512 ; Par défaut : 32) La taille réelle du paquet est supérieure de huit octets à la taille spécifiée étant donné que le commutateur ajoute des informations d'en-tête.

Configuration par défaut

Cette commande ne possède aucune valeur par défaut pour l'hôte.

Mode de commande

Normal Exec, Privileged Exec

Utilisation de la commande

- Utilisez la commande « ping » pour voir s'il est possible d'atteindre un autre site du réseau.
- Les éléments suivants sont des résultats de la commande ping :
  - Normal response : La réponse normale survient entre une et dix secondes plus tard, selon le trafic réseau.
  - Destination does not respond : Si l'hôte ne répond pas, le commutateur affiche « timeout ».
  - Destination unreachable : La passerelle de cette destination indique que la destination n'est pas accessible.
  - Network or host unreachable : La passerelle n'a trouvé aucune entrée correspondante dans la table de routage.
- Appuyez sur <Esc> pour mettre un terme au ping.

Exemple

```
Console#ping 10.1.0.19
Type Ctrl-C to abort.
PING to 10.1.0.19, by 5 32-byte payload ICMP packets, timeout is 5
seconds
response time: 0 ms
response time: 0 ms
response time: 10 ms
response time: 10 ms
response time: 10 ms
Ping statistics for 10.1.0.19:
 5 packets transmitted, 5 packets received (100%), 0 packets lost (0%)
Approximate round trip times:
 Minimum = 0 ms, Maximum = 10 ms, Average = 6 ms
Console#
```

4.3.7.8 ip filter

Cette commande permet d'empêcher des paquets IP spécifiés d'atteindre le port de gestion interne depuis les ports à liaison descendante. Utilisez la forme **no** pour supprimer une règle de la table de filtrage.

Syntaxe

ip filter [*rule-number*] *action protocol* {*source source-bitmask*} {*destination destination-bitmask*} [**fragments**] [**log**]

Le numéro du port n'est pas vérifié. L'option **fragments** est autorisée.

ip filter [*rule-number*] *action protocol* {*source source-bitmask*} [*source-port-range*] {*destination destination-bitmask*} [*destination-port-range*] [**log**]

Le numéro du port est vérifié ; en d'autres termes, si *source-port-range* ou *destination-port-range* est spécifié, l'option **fragments** n'est pas autorisée.

ip filter [*rule-number*] *action* **tcp** {*source source-bitmask*} [*source-port-range*] {*destination destination-bitmask*} [*destination-port-range*] [**code** {{*code code-bitmask*} | *code-keyword-seq*}] [**log**]

Recherche le mot-clé **tcp**. Si elle le trouve, l'option **code** est autorisée.

no ip filter {**all** |*rule-number*}

Supprime le numéro de règle spécifié de la table de filtrage.

- *rule-number* : Insère une règle de filtrage à l'emplacement spécifié de la table, repoussant d'un rang les motifs existants à cet emplacement, ou sous celui-ci, dans la table. Un numéro de règle ne peut pas dépasser le numéro suivant affiché dans la table. Si le numéro de la règle n'est pas spécifié, un nouveau motif est ajouté à la fin de la table des règles. Le nombre maximal de règles est de 128.
- *action* - {**deny** | **permit**}
  Empêche ou autorise le passage des paquets entre les ports à liaison descendante et le port de gestion.
- *protocol* - {**any** | **tcp** | **udp** | *number*}
  Indique un protocole (TCP, UDP, Any) ou un numéro de protocole spécifique (0-255).
- *source source-bitmask :* L'adresse source de la trame et le masque de réseau.
- *source-port-range* - [*number* | *start_number-end_number*]
  Port source TCP/UDP ou plage de ports. (Plage : 0-65535)
- *destination destination-bitmask :* Adresse de destination de la trame et masque de réseau.
- *destination-port-range* - [*number* | *start_number-end_number*]
  Port de destination TCP/UDP ou plage de ports. (Plage : 0-65535)
- **code**
  - *code* : Nombre décimal (représentant une chaîne de bits) spécifiant un code à l'octet 14 de l'en-tête TCP. (Plage : 0-63)
  - *code-bitmask* : Nombre décimal (représentant un masque de bits) appliqué au code. Entrez un nombre décimal, où l'équivalent binaire « 1 » signifie une correspondance avec un bit et « 0 » signifie qu'un bit est ignoré. Il est possible de spécifier les bits suivants :
    - 1 (fin) - Finish
    - 2 (syn) - Synchronize
    - 4 (rst) - Reset
    - 8 (psh) - Push
    - 16 (ack) - Acknowledgement
    - 32 (urg) - Urgent pointer
  - *code-keyword-seq* : Les mots-clés de code suivants peuvent être spécifiés, mais doivent suivre la séquence indiquée : **fin** | **syn** | **rst** | **psh** | **ack** | **urg** (Le mot-clé du code doit être ACTIVÉ en cas de spécification et DÉSACTIVÉ en cas de non-spécification.)

- **fragments** : La règle ne recherche que les paquets avec le bit MF (More Fragments) actif ou avec un écart de fragments supérieur à zéro. Si l'option **fragment** n'est pas définie, la règle recherche à la fois les fragments et les paquets non fragmentés.
- **log** : Consigne tous les paquets correspondants dans le tampon de journalisation. Le nombre maximal d'entrées enregistrées dans ce tampon est de 64. Lorsque le tampon est plein, il revient au début et écrase les entrées les plus anciennes. Remarquez que le journal est enregistré dans la RAM et qu'il s'efface lorsque le commutateur est réinitialisé.

Configuration par défaut

Aucune

Mode de commande

General Configuration

Utilisation de la commande

- Par défaut, le système arrête tous les paquets IP passant des ports à liaison descendante au port de gestion (NETMGT). Si les serveurs Blade doivent pouvoir accéder au réseau de gestion par le biais du port de gestion (NETMGT), vous devez définir un filtre autorisant des trames spécifiques à passer entre les ports à liaison descendante et le port de gestion. Remarquez que le trafic ne peut jamais passer des ports à liaison ascendante au port de gestion.
- Un fragment est un paquet où MF (more fragments) = 1 ou Fragment Offset > 0. Si le mot-clé **fragments** est absent d'une règle, alors les fragments et les paquets non fragmentés seront contrôlés par la règle.
- Lorsque vous spécifiez une valeur de code et un masque, la logique réside dans le fait qu'un paquet correspond si <value in header> & <mask> == <value> & <mask>. Par exemple, utilisez la valeur de code et le masque affichés ci-dessous pour attraper des paquets avec les indicateurs suivants activés :
  - Code SYN valable, utilisez « code 2 2 »
  - SYN et ACK valables, utilisez « code 18 18 »
  - SYN valable et ACK non valable, utilisez « code 2 18 »

Exemple - Filtrage d'adresses

Cet exemple permet à tous les paquets de passer par le filtre en autorisant tous les types de protocoles et une adresse et un masque de réseau nuls tant pour l'adresse source que pour l'adresse de destination.

```
Console(config)#ip filter permit any 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
Console(config)#
```

Dans ce cas, tous les paquets entrants sont acceptés si l'adresse source se trouve sur le sous-réseau 10.7.1.x. Par exemple, s'il y a correspondance avec la règle ; à savoir si la règle (10.7.1.1 & 255.255.255.0) est égale à l'adresse masquée (10.7.1.2 & 255.255.255.0), le paquet passe.

```
Console(config)#ip filter permit any 10.7.1.1 255.255.255.0 0.0.0.0
   0.0.0.0
Console(config)#
```

Exemple - Recherche de fragments

Cet exemple bloque tous les fragments et consigne les paquets correspondants dans le journal.

```
Console(config)#ip filter deny any 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
   fragment log
Console(config)#
```

Exemple - Recherche de valeurs de code

Cet exemple bloque tous les paquets TCP des adresses de classe C 192.168.1.0 avec SYN actif.

```
Console(config)#ip filter deny tcp 192.168.1.0 255.255.255.0 0.0.0.0
   0.0.0.0 code syn
Console(config)#
```

Cet exemple bloque également tous les paquets TCP des adresses de classe C 192.168.1.0 avec SYN actif.

```
Console(config)#ip filter deny tcp 192.168.1.0 255.255.255.0 0.0.0.0
   0.0.0.0 code 2 2
Console(config)#
```

Exemple - Recherche de numéros de port

Cet exemple autorise le passage des paquets TCP des adresses de classe C 192.168.1.0 vers toutes les destinations lorsqu'ils sont configurés pour le port de destination 80.

```
Console(config)#ip filter permit tcp 192.168.1.0 255.255.255.0 0.0.0.0
   0.0.0.0 80
Console(config)#
```

Cet exemple abandonne tous les paquets TCP de la source 10.7.1.1 vers la destination 10.8.1.1, avec le port source situé entre 30 et 46, et le port de destination entre 100 et 2000.

```
Console(config)#ip filter deny tcp 10.7.1.1 255.255.255.255 30-46
   10.8.1.1 255.255.255.255 100-2000
Console(config)#
```

4.3.7.9 show ip filter

Cette commande permet d'afficher toutes les règles dans la table de filtrage IP.

Syntaxe

show ip filter [*rule-number* | **log**]

- *rule-number* : Affichez une règle de filtrage à l'endroit spécifié dans le tableau. Plage : 1-128
- **log** : Affiche tous les paquets enregistrés dans le tampon de journalisation. Remarquez que les paquets enregistrés dans ce tampon doivent correspondre aux règles de la table de filtrage. Le nombre maximal d'entrées enregistrées dans le tampon est de 64.

Si aucune option n'est sélectionnée, tous les paquets du tampon sont affichés.

Configuration par défaut

Aucune

Mode de commande

Privileged Exec

Exemple

Dans ce cas, la seule règle spécifiée autorise les paquets du sous-réseau 10.1.0.x à passer entre le port de gestion et les ports à liaison descendante.

```
Console#show ip filter
Ip filter:
 Rule:1, Action: permit, Protocol: any, Log: disable, Fragments: disable
 Source: 10.1.0.0 255.255.255.0 any
 Destination: 10.1.0.0 255.255.255.0 any
```

4.3.8 Commandes d'interface

Ces commandes permettent d'afficher et de définir des paramètres de communication pour un port Ethernet, une liaison groupée ou un VLAN.

Commande	Fonction	Mode	Page
interface	Configure un type d'interface et passe en mode de configuration d'interface.	GC	4-74
description	Ajoute une description à une configuration d'interface.	IC	4-75
speed-duplex	Configure la vitesse et le mode duplex d'une interface donnée lorsque l'auto-négociation est désactivée.	IC	4-75
negotiation	Active l'auto-négociation pour une interface donnée.	IC	4-77
capabilities	Publie les capacités d'une interface donnée afin de les utiliser dans le cadre de l'auto-négociation.	IC	4-78
flowcontrol	Active le contrôle de flux pour une interface donnée.	IC	4-79
shutdown	Désactive une interface.	IC	4-80
switchport broadcast packet-rate	Définit le seuil de contrôle des orages de diffusion.	IC	4-81
clear counters	Efface les statistiques d'une interface.	PE	4-82
show interfaces status	Affiche l'état de l'interface spécifiée.	NE, PE	4-83
show interfaces counters	Affiche les statistiques de l'interface spécifiée.	NE, PE	4-84
show interfaces switchport	Affiche l'état administratif et opérationnel d'une interface.	NE, PE	4-85

4.3.8.1 interface

Cette commande permet de configurer un type d'interface et de passer en mode de configuration d'interface.

Syntaxe

interface *interface*
no interface port-channel *channel-id*

interface

- **ethernet** *port-name*
  port-name : liaison descendante : SNP0-15 ; liaison ascendante : NETP0-7 ; gestion : NETMGT
- **port-channel** *channel-id* (Plage : 1-6)
- **vlan** *vlan-id* (Plage : 1-4094)

Configuration par défaut

Aucune

Mode de commande

Global Configuration

Exemple

Pour spécifier le premier port à liaison ascendante, entrez la commande suivante :

```
Console(config)#interface ethernet NETP0
Console(config-if)#
```

4.3.8.2 description

Cette commande permet d'ajouter une description à une interface. Utilisez la forme **no** pour supprimer la description.

Syntaxe

description *string*
no description

string : Commentaire ou description vous permettant de vous rappeler les éléments connectés à cette interface. (Plage : 1-64 caractères)

Configuration par défaut

NETP0-7 : Connecteur RJ-45 externe NET0-7
SNP0-15 : Emplacement du serveur Blade 0 à 15
NETMGT : Connecteur RJ-45 externe NETMGT

Mode de commande

Interface Configuration (Ethernet, Port Channel)

Exemple

L'exemple suivant configure une description pour le port à liaison descendante SNP5.

```
Console(config)#interface ethernet SNP5
Console(config-if)#description RD-SW#3
Console(config-if)#
```

4.3.8.3 speed-duplex

Cette commande permet de configurer la vitesse et le mode duplex d'une interface donnée lorsque l'auto-négociation est désactivée. Utilisez la forme **no** pour restaurer la valeur par défaut.

Syntaxe

speed-duplex {**1000full** | **100full** | **100half** | **10full** | **10half**}
no speed-duplex

- **1000full** : Force un fonctionnement en semi duplex à 1000 Mbps.
- **1000full** : Force un fonctionnement en full duplex à 100 Mbps.
- **100half** : Force un fonctionnement en semi duplex à 100 Mbps
- **10full** : Force un fonctionnement en full duplex à 10 Mbps.
- **10half** : Force un fonctionnement en semi duplex à 10 Mbps

Configuration par défaut

- L'auto-négociation est activée par défaut.
- Lorsque l'auto-négociation est désactivée, le paramètre speed-duplex est 100full pour les ports Fast Ethernet et 1000full pour les ports Gigabit Ethernet.

Remarque - Lorsque l'auto-négociation est désactivée, vous pouvez uniquement définir les ports à liaison ascendante à 10 Mbps ou 100 Mbps. Pour forcer un port à fonctionner à 1 Gbps en duplex, activez l'auto-négociation et définissez les capacités du port à « 1000full » uniquement.

Mode de commande

Interface Configuration (Ethernet, Port Channel)

Utilisation de la commande

- Pour forcer le fonctionnement à la vitesse et au mode duplex spécifiés dans une commande **speed-duplex**, utilisez la commande **no negotiation** pour désactiver l'auto-négociation sur l'interface sélectionnée. Cependant, remarquez que l'auto-négociation ne peut pas être désactivée sur les ports à liaison descendante. Ces ports fonctionnent à 1000 Mbps en mode duplex.
- Lorsque vous utilisez la commande **negotiation** pour activer l'auto-négociation, les paramètres optimaux sont déterminées par la commande **capabilities**. Pour définir la vitesse/le mode duplex sous auto-négociation, le mode requis doit être spécifié dans la liste des capacités pour une interface.

Exemple

L'exemple suivant configure le port NETP5 à 100 Mbps en mode semi duplex.

```
Console(config)#interface ethernet NETP5
Console(config-if)#no negotiation
Console(config-if)#speed-duplex 100half
Console(config-if)#
```

Commandes associées

negotiation (4-77)
capabilities (4-78)

4.3.8.4 negotiation

Cette commande permet d'activer l'auto-négociation pour une interface donnée. Utilisez la forme **no** pour désactiver l'auto-négociation.

Syntaxe

negotiation
no negotiation

Configuration par défaut

Activée

Mode de commande

Interface Configuration (Ethernet, Port Channel)

Utilisation de la commande

- Les ports à liaison descendante SNP0-15 sont fixes ; l'auto-négociation est désactivée.
- Lorsque l'auto-négociation est activée, le commutateur négocie les meilleurs paramètres pour une liaison sur la base de la commande **capabilites**. Lorsque l'auto-négociation est désactivée, vous devez spécifier manuellement les attributs de liaison à l'aide des commandes **speed-duplex** et **flowcontrol**.
- Si l'auto-négociation est désactivée, la configuration du signal auto-MDI/MDI-X est également désactivée pour les ports à liaison ascendante.

Exemple

L'exemple suivant configure le port SNP11 afin que celui-ci utilise l'auto-négociation.

```
Console(config)#interface ethernet SNP11
Console(config-if)#negotiation
Console(config-if)#
```

Commandes associées

capabilities (4-78)
speed-duplex (4-75)
flowcontrol (4-79)

4.3.8.5 capabilities

Cette commande permet de publier les capacités des ports pour une interface donnée pendant l'auto-négociation. Utilisez la forme **no** avec les paramètres afin de supprimer une capacité publiée ou la forme **no** sans les paramètres pour restaurer les valeurs par défaut.

Syntaxe

capabilities {**1000full** | **100full** | **100half** | **10full** | **10half** | **flowcontrol** | **symmetric**}
no port-capabilities [**1000full** | **100full** | **100half** | **10full** | **10half** | **flowcontrol** | **symmetric**]

- 1000full : Prend en charge le fonctionnement en duplex à 1000 Mbps
- 100full : Prend en charge le fonctionnement en duplex à 100 Mbps
- 100half : Prend en charge le fonctionnement en semi duplex à 100 Mbps
- 10full : Prend en charge le fonctionnement en duplex à 10 Mbps
- 10half : Prend en charge le fonctionnement en semi duplex à 10 Mbps
- flowcontrol : Prend en charge le contrôle de flux
- symmetric (Gigabit uniquement) : Cochez cette option pour transmettre et recevoir des trames de pause ou décochez-la pour activer l'auto-négociation de l'émetteur et du récepteur pour les trames de pause asymétriques. (*Le commutateur ASIC courant ne prend en charge que les trames de pause symétriques.*)

Configuration par défaut

NETMGT : 10half, 10full, 100half, 100full
NETP0-7 : 10half, 10full, 100half, 100full, 1000full, flow control
SNP0-15 : 1000full

Mode de commande

Interface Configuration (Ethernet, Port Channel)

Utilisation de la commande

- Les capacités des ports à liaison descendante SNP0-15 sont fixées à 1000full.
- Les capacités des ports à liaison ascendante NETP0-7 comprennent 10half, 10full, 100half, 100full, 1000full, flowcontrol et symmetric. Lorsque l'auto-négociation est activée avec la commande **negotiation**, le commutateur négocie les meilleurs paramètres pour une liaison basée sur la commande **capabilites**. Lorsque l'auto-négociation est désactivée, vous devez spécifier manuellement les attributs de liaison à l'aide des commandes **speed-duplex** et **flowcontrol**.
- Les capacités des ports NETMGT sont fixées à 10half, 10full, 100half, 100full.

Exemple

L'exemple suivant configure le port NETP5 à 100half, 100full et flow control.

```
Console(config)#interface ethernet NETP5
Console(config-if)#no capabilities 10half
Console(config-if)#no capabilities 10hfull
Console(config-if)#no capabilities 1000full
Console(config-if)#capabilities 100half
Console(config-if)#capabilities 100full
Console(config-if)#capabilities flowcontrol
Console(config-if)#
```

Commandes associées

negotiation (4-77)
speed-duplex (4-75)
flowcontrol (4-79)

4.3.8.6 flowcontrol

Cette commande permet d'activer le contrôle de flux. Utilisez la forme **no** pour désactiver le contrôle de flux.

Remarque - Les commutateurs intégrés sur le châssis Sun Fire™ B1600 pour serveurs Blade sont chacun composés de deux puces de commutateurs reliées. Il n'est possible d'activer le contrôle du flux qu'entre deux ports situés sur la même puce. Les ports NETP0 à NETP3 et SNP0 à SNP7 se trouvent sur l'une des puces. Les ports NETP4 à NETP7 et SNP8 à SNP15 se trouvent sur l'autre.

Syntaxe

flowcontrol
no flowcontrol

Configuration par défaut

Contrôle de flux activé

Mode de commande

Interface Configuration (Ethernet, Port Channel)

Utilisation de la commande

- Le contrôle du flux peut empêcher la perte de trames en « bloquant » le trafic depuis les stations ou les segments terminaux connectés directement au commutateur lorsque son tampon se remplit. En cas d'activation, une contre-pression est utilisée pour le fonctionnement en semi duplex et IEEE802.3x pour un fonctionnement en duplex.
- Pour forcer l'activation ou la désactivation du contrôle de flux (à l'aide des commandes **flowcontrol** ou no **flowcontrol**) utilisez la commande **no negotiation** pour désactiver l'auto-négociation sur l'interface sélectionnée.
- Lorsque vous utilisez la commande **negotiation** pour activer l'auto-négociation, les paramètres optimaux sont déterminées par la commande **capabilities**. Pour activer le contrôle de flux sous auto-négociation, « flowcontrol » doit être inclus dans la liste des capacités de l'un des ports.
- Evitez d'utiliser le contrôle de flux sur un port connecté à un concentrateur, à moins que cela ne soit nécessaire pour résoudre un problème. Sinon, les signaux de blocage de la contre-pression peuvent amoindrir les performances globales du segment raccordé au concentrateur).

Exemple

L'exemple suivant active le contrôle de flux sur le port NETP7.

```
Console(config)#interface ethernet NETP7
Console(config-if)#flowcontrol
Console(config-if)#no negotiation
Console(config-if)#
```

Commandes associées

negotiation (4-77)
capabilities (flowcontrol, symmetric) (4-78)

4.3.8.7 shutdown

Cette commande permet de désactiver une interface. Pour redémarrer une interface désactivée, utilisez la forme **no**.

Syntaxe

shutdown
no shutdown

Configuration par défaut

Toutes les interfaces sont activées.

Mode de commande

Interface Configuration (Ethernet, Port Channel)

Utilisation de la commande

Cette commande permet de désactiver un port en cas de comportement anormal (par exemple, un nombre de collision excessif), puis de le réactiver une fois le problème résolu. Vous pouvez également désactiver un port pour des raisons de sécurité.

Exemple

L'exemple suivant désactive le port Ethernet SNP5.

```
Console(config)#interface ethernet SNP5
Console(config-if)#shutdown
Console(config-if)#
```

4.3.8.8 switchport broadcast packet-rate

Cette commande permet de configurer le contrôle des orages de diffusion. Utilisez la forme **no** pour désactiver le contrôle des orages de diffusion.

Syntaxe

switchport broadcast packet-rate *rate*
no switchport broadcast

rate : Niveau du seuil exprimé en temps que taux (à savoir en paquets par seconde). (Plage : 16, 64, 128, 256)

Configuration par défaut

Activé pour tous les ports
256 paquets par seconde

Mode de commande

Interface Configuration (Ethernet)

Utilisation de la commande

- Lorsque le trafic de diffusion dépasse le seuil spécifié, les paquets « en trop » sont abandonnés.
- Cette commande permet d'activer ou de désactiver le contrôle des orages de diffusion pour l'interface sélectionnée. Toutefois, la valeur seuil spécifiée s'applique à l'ensemble du commutateur.
- Les ports à liaison descendante SNP0-15 sont fixes ; le contrôle des orages de diffusion est désactivé.

Exemple

L'exemple suivant montre comment configurer un contrôle de diffusion à 64 paquets par seconde :

```
Console(config)#interface ethernet SNP5
Console(config-if)#switchport broadcast packet-rate 64
Console(config-if)#
```

Remarque - Notez que la commande **switchport broadcast** active le contrôle des orages de diffusion sur l'interface spécifiée, mais qu'elle définit le seuil de diffusion pour toutes les interfaces du commutateur.

4.3.8.9 clear counters

Cette commande permet d'effacer les statistiques d'une interface.

Syntaxe

clear counters *interface*

interface - **ethernet** *port-name*
port-name : liaison descendante : SNP0-15 ; liaison ascendante : NETP0-7 ; gestion : NETMGT

Configuration par défaut

Aucune

Mode de commande

Privileged Exec

Utilisation de la commande

Les statistiques ne sont réinitialisées qu'au redémarrage du système. Cette commande remet à zéro la valeur de base des statistiques affichées pour la session de gestion courante. Toutefois, si vous vous déconnectez et vous reconnectez à l'interface de gestion, les statistiques affichées indiquent la valeur absolue cumulée depuis le dernier redémarrage du système.

Exemple

L'exemple suivant efface les statistiques du port SNP5.

```
Console#clear counters ethernet SNP5
Console#
```

4.3.8.10 show interfaces status

Cette commande permet d'afficher l'état d'une interface.

Syntaxe

show interfaces status [*interface*]

interface

- **ethernet** *port-name*
  port-name : liaison descendante : SNP0-15 ; liaison ascendante : NETP0-7 ; gestion : NETMGT
- **port-channel** *channel-id* (Plage : 1-6)
- **vlan** *vlan-id* (Plage : 1-4094)

Configuration par défaut

Affiche l'état de toutes les interfaces.

Mode de commande

Normal Exec, Privileged Exec

Utilisation de la commande

Si aucune interface n'est spécifiée, des informations relatives à toutes les interfaces s'affichent. Pour une description des éléments affichés par cette commande, reportez-vous à « Affichage de l'état de la connexion » à la page 3-80.

Exemple

```
Console#show interfaces status ethernet SNP11
Information of SNP11
Basic information:
  Port type: 1000SX
  Mac address: 00-00-e8-00-00-0a
 Configuration:
  Name: Blade Slot 11
  Port admin status: Up
Speed-duplex: Auto
  Capabilities: 1000full,
Broadcast storm status: Enabled
  Broadcast storm limit: 256 packets/second
  Flow control status: Enabled
  Lacp status: Disabled
 Current status:
  Link status: Down
  Operation speed-duplex: 1000full
  Flow control type: Dot3X
Console#
```

4.3.8.11 show interfaces counters

Cette commande permet d'afficher les statistiques d'une interface.

Syntaxe

show interfaces counters [*interface*]

interface

- **ethernet** *port-name*
  port-name : liaison descendante : SNP0-15 ; liaison ascendante : NETP0-7 ; gestion : NETMGT
- **port-channel** *channel-id* (Plage : 1-6)

Configuration par défaut

Affiche les compteurs de toutes les interfaces.

Mode de commande

Normal Exec, Privileged Exec

Utilisation de la commande

Si aucune interface n'est spécifiée, des informations relatives à toutes les interfaces s'affichent. Pour une description des éléments affichés par cette commande, reportez-vous à « Affichage des statistiques du port » à la page 3-118.

Exemple

```
Console#show interfaces counters ethernet NETP7
NETP7:
 Iftable stats:
  Octets input: 19648, Octets output: 714944
  Unicast input: 0, Unicast output: 0
  Discard input: 0, Discard output: 0
  Error input: 0, Error output: 0
  Unknown protos input: 0, QLen output: 0
 Extended iftable stats:
  Multi-cast input: 0, Multi-cast output: 10524
  Broadcast input: 136, Broadcast output: 0
Ether-like stats:
  Alignment errors: 0, FCS errors: 0
  Single Collision frames: 0, Multiple collision frames: 0
  SQE Test errors: 0, Deferred transmissions: 0
  Late collisions: 0, Excessive collisions: 0
  Internal mac transmit errors: 0, Internal mac receive errors: 0
  Frame too longs: 0, Carrier sense errors: 0
RMON stats:
  Drop events: 0, Octets: 734720, Packets: 10661
  Broadcast pkts: 136, Multi-cast pkts: 10525
  Undersize pkts: 0, Oversize pkts: 0
  Fragments: 0, Jabbers: 0
  CRC align errors: 0, Collisions: 0
  Packet size <= 64 octets: 9877, Packet size 65 to 127 octets: 93
  Packet size 128 to 255 octets: 691, Packet size 256 to 511 octets: 0
  Packet size 512 to 1023 octets: 0, Packet size 1024 to 1518 octets: 0
Console#
```

4.3.8.12 show interfaces switchport

Cette commande permet d'afficher les paramètres de configuration d'interface avancés.

Syntaxe

show interfaces switchport [*interface*]

interface

- **ethernet** *port-name*
  port-name : liaison descendante : SNP0-15 ; liaison ascendante : NETP0-7 ; gestion : NETMGT
- **port-channel** *channel-id* (Plage : 1-6)

Configuration par défaut

Affiche toutes les interfaces

Mode de commande

Normal Exec, Privileged Exec

Utilisation de la commande

Si aucune interface n'est spécifiée, des informations relatives à toutes les interfaces apparaissent. Les éléments affichés par cette commande comprennent :

- **Broadcast threshold** : Indique si le contrôle des orages de diffusion est activé ou désactivé ; s'il est activé, indique également son seuil (page 4-81).
- **Lacp status** : Indique si le protocole LACP (Link Aggregation Control Protocol) a été activé ou désactivé (page 4-147).
- **VLAN membership mode** : Indique le mode d'appartenance (Trunk (Groupe) ou Hybrid (Hybride)) (page 4-108).
- **Ingress rule** : Indique si le filtrage à l'entrée est activé ou désactivé (page 4-110).
- **Acceptable frame type** : Indique si les trames VLAN acceptables comprennent toutes les trames ou seulement celles qui sont marquées (page 4-109).
- **Native VLAN** : Indique l'identificateur du VLAN du port par défaut (page 4-111).
- **Priority for untagged traffic** : Indique la priorité par défaut pour les trames non marquées (page 4-133).
- **Gvrp status** : Indique si le protocole (GARP VLAN Registration Protocol) est activé ou désactivé (page 4-115).
- **Allowed Vlan** : Indique les VLAN auxquels est associée cette interface. « (u) » signifie « non marqué » et « (t) » signifie « marqué » (page 4-112).
- **Forbidden Vlan** : Indique les VLAN auxquels cette interface ne peut pas être associée de manière dynamique via le GVRP (page 4-113).

Exemple

Cet exemple montre la configuration du port Ethernet NETP7.

```
Console#show interfaces switchport ethernet NETP7
Information of NETP7
 Broadcast threshold: Enabled, 256 packets/second
 Lacp status: Enabled
 VLAN membership mode: Hybrid
 Ingress rule: Disabled
 Acceptable frame type: All frames
 Native VLAN: 1
 Priority for untagged traffic: 0
 Gvrp status: Enabled
 Allowed Vlan:    1(u),
 Forbidden Vlan:    2,
Console#
```

4.3.9 Commandes de la table d'adressage

Ces commandes permettent de configurer la table d'adressage dans le but de filtrer les adresses spécifiées, d'afficher les entrées courantes, d'effacer la table ou de définir le délai d'obsolescence.

Commande	Fonction	Mode	Page
mac-address-table static	Affecte une adresse statique à un port sur un VLAN	GC	4-87
clear mac-address-table dynamic	Supprime les entrées apprises de la base de données de transmission	PE	4-88
show mac-address-table	Affiche les entrées de la base de données de transmission du pont	PE	4-88
mac-address-table aging-time	Définit le délai d'obsolescence de la table d'adressage	GC	4-89
show mac-address-table aging-time	Affiche le délai d'obsolescence de la table d'adressage	PE	4-90

4.3.9.1 mac-address-table static

Cette commande permet d'affecter une adresse statique à un port de destination. Utilisez la forme **no** pour supprimer une adresse.

Syntaxe

mac-address-table static *mac-address* {**interface** *interface*} **vlan** *vlan-id* [*action*]
no mac-address-table static *mac-address* **vlan** *vlan-id*

- *mac-address* : Adresse MAC.
- *interface*
  - **ethernet** *port-name*
    port-name : liaison descendante : SNP0-15 ; liaison ascendante : NETP0-7 ; gestion : NETMGT
  - **port-channel** *channel-id* (Plage : 1-6)
- *vlan-id* : identificateur du VLAN (Plage : 1-4094)
- *action* :
  - **permanent** : L'affectation est permanente.
  - **delete-on-reset** : L'affectation dure jusqu'à la réinitialisation du commutateur.

Configuration par défaut

Aucune adresse statique n'est définie. Le mode par défaut est permanent.

Mode de commande

Global Configuration

Utilisation de la commande

- L'adresse statique d'un périphérique hôte peut être affectée à un port spécifique sur un VLAN spécifique. Cette commande permet d'ajouter des adresses statiques à une table d'adressage MAC. Les adresses statiques présentent les caractéristiques suivantes :
  - Elles ne sont pas supprimées de la table d'adressage quand la liaison à une interface donnée est interrompue.
  - Elles sont liées à l'interface affectée et ne sont pas déplacées. Lorsqu'une adresse statique est détectée sur une autre interface, l'adresse est ignorée et n'est pas inscrite dans la table d'adressage.
  - Une adresse statique ne peut pas être apprise sur un autre port tant qu'elle n'a pas été supprimée à l'aide de la forme **no** de cette commande.

Exemple

```
Console(config)#mac-address-table static 00-e0-29-94-34-de
ethernet SNP1 vlan 1 delete-on-reset
Console(config)#
```

4.3.9.2 clear mac-address-table dynamic

Cette commande permet de supprimer toutes les entrées apprises de la base de données de transmission et de réinitialiser les compteurs d'émissions et de réceptions pour les entrées statiques ou configurées par le système.

Configuration par défaut

Aucune

Mode de commande

Privileged Exec

Exemple

```
Console#clear mac-address-table dynamic
Console#
```

4.3.9.3 show mac-address-table

Cette commande permet d'afficher les classes d'entrées dans la base de données de transmission du pont.

Syntaxe

show mac-address-table [**address** *mac-address* [*mask*]] [**interface** *interface*] [**vlan** *vlan-id*] [**sort** {**address** | **vlan** | **interface**}]

- *mac-address* : Adresse MAC.
- *mask* : Bits à ignorer dans l'adresse.
- *interface*
  - **ethernet** *port-name*
    port-name : liaison descendante : SNP0-15 ; liaison ascendante : NETP0-7 ; gestion : NETMGT
  - **port-channel** *channel-id* (Plage : 1-6)
- *vlan-id* : Identificateur du VLAN (Plage : 1-4094)
- **sort** : Tri par adresse, VLAN ou interface.

Configuration par défaut

Aucune

Mode de commande

Privileged Exec

Utilisation de la commande

La table d'adressage MAC contient les adresses MAC associées à chaque interface. Remarquez que la zone Type peut inclure les types suivants :

- Learned : entrées d'adressage dynamiques
- Permanent : entrée statique
- Delete-on-reset : entrée statique à supprimer lorsque le système est réinitialisé

Exemple

```
Console#show mac-address-table
Interface Mac Address       Vlan Type
 --------- ----------------- ---- -----------------
     SNP11 00-10-b5-62-03-74    1 Learned
Console#
```

4.3.9.4 mac-address-table aging-time

Cette commande permet de définir le délai d'obsolescence des entrées de la table d'adressage. Utilisez la forme **no** pour restaurer le délai d'obsolescence par défaut.

Syntaxe

mac-address-table aging-time *seconds*
no mac-address-table aging-time

seconds : Délai en secondes (18-2184).

Configuration par défaut

300 secondes

Mode de commande

Global Configuration

Utilisation de la commande

Le délai d'obsolescence sert à supprimer les informations de transmission apprises de manière dynamique après un délai prédéfini.

Exemple

```
Console(config)#mac-address-table aging-time 300
Console(config)#
```

4.3.9.5 show mac-address-table aging-time

Cette commande permet d'afficher le délai d'obsolescence des entrées de la table d'adressage.

Configuration par défaut

Aucune

Mode de commande

Privileged Exec

Exemple

```
Console#show mac-address-table aging-time
 Aging time: 300 sec.
Console#
```

4.3.10 Commandes de sécurité des ports

Ces commandes permettent de désactiver la fonction d'apprentissage ou de spécifier manuellement des adresses sécurisées pour un port. Il se peut que vous souhaitiez laisser la sécurité des ports désactivée (et donc activer la fonction d'apprentissage) pendant une période initiale afin d'enregistrer tous les membres courants du VLAN du port sélectionné, puis activer la sécurité des ports pour vous assurer que le port abandonne toutes les trames entrantes présentant une adresse MAC source inconnue ou préalablement détectée sur un autre port.

Commande	Fonction	Mode	Page
port security	Configure un port sécurisé	IC	4-91
mac-address-table static	Affecte une adresse statique à un port sur un VLAN	GC	4-87
show mac-address-table	Affiche les entrées de la base de données de transmission du pont	PE	4-88

4.3.10.1 port security

Cette commande permet de configurer un port sécurisé. Utilisez la forme **no** pour désactiver la sécurité des ports.

Syntaxe

port security
no port security

Configuration par défaut

La sécurité des ports est désactivée partout.

Mode de commande

Interface Configuration (Ethernet)

Utilisation de la commande

- Si vous activez la sécurité du port, le commutateur cesse l'apprentissage dynamique de nouvelles adresses sur le port spécifié. Seul le trafic entrant avec des adresses source déjà enregistrées dans la table d'adressage statique ou dynamique est accepté.
- Pour utiliser la sécurité des ports, autorisez d'abord le commutateur à apprendre dynamiquement <l'adresse MAC source, la >paire VLAN pour les trames reçues sur un port dans un premier temps, puis activez la sécurité des ports pour cesser l'apprentissage des adresses. Veillez à activer la fonction d'apprentissage suffisamment longtemps pour vous assurer que tous les membres VLAN valables ont été enregistrés sur le port sélectionné.
- Pour ajouter de nouveaux membres VLAN ultérieurement, vous pouvez ajouter manuellement des adresses sécurisées à l'aide de la commande **mac-address-table static**, ou désactivez la sécurité des ports pour réactiver la fonction d'apprentissage suffisamment longtemps pour que les nouveaux membres VLAN soient enregistrés. Si vous le souhaitez, vous pouvez alors désactiver l'apprentissage une nouvelle fois, à des fins de sécurité.
- Un port sécurisé présente les restrictions suivantes :
  - utilisation de la surveillance du port impossible ;
  - fonctionnement en tant que port multi-VLAN impossible ;
  - connexion à un périphérique d'interconnexion réseau impossible ;
  - fonctionnement en tant que port de groupe impossible.

Exemple

L'exemple suivant active la sécurité du port SNP5 :

```
Console(config)#interface ethernet SNP5
Console(config-if)#port security
```

Commandes associées

mac-address-table static (4-87)
show mac-address-table (4-88)

4.3.11 Commandes du Spanning Tree

Cette section comprend des commandes qui configurent l'algorithme Spanning Tree (STA) pour le commutateur dans son ensemble, et des commandes qui configurent le STA pour l'interface sélectionnée.

Commande	Fonction	Mode	Page
spanning-tree	Active le protocole Spanning Tree	GC	4-93
spanning-tree mode	Configure le mode STP ou RSTP	GC	4-94
spanning-tree forward-time	Configure le délai de transmission du pont Spanning Tree	GC	4-95
spanning-tree hello-time	Configure le délai de connexion du pont Spanning Tree	GC	4-96
spanning-tree max-age	Configure l'âge maximum du pont Spanning Tree	GC	4-96
spanning-tree priority	Configure la priorité du pont Spanning Tree	GC	4-97
spanning-tree path-cost method	Configure la méthode de la distance à parcourir pour le RSTP	GC	4-98
spanning-tree transmission-limit	Configure la limite de transmission pour le RSTP	GC	4-98
spanning-tree cost	Configure la distance à parcourir Spanning Tree d'une interface	IC	4-99
spanning-tree port-priority	Configure la priorité Spanning Tree d'une interface	IC	4-100
spanning-tree edge-port	Active la transmission rapide pour les ports de périphérie	IC	4-101
spanning-tree protocol-migration	Réactive le format BPDU approprié	PE	4-102
spanning-tree link-type	Configure le type de liaison pour le RSTP	IC	4-102
show spanning-tree	Affiche la configuration du Spanning Tree	PE	4-103

4.3.11.1 spanning-tree

Cette commande permet d'activer l'algorithme Spanning Tree globalement pour ce commutateur. Utilisez la forme **no** pour désactiver cette fonction.

Syntaxe

spanning-tree
no spanning-tree

Configuration par défaut

Le Spanning Tree est activé.

Mode de commande

Global Configuration

Utilisation de la commande

L'algorithme Spanning Tree peut être utilisé pour détecter et désactiver les boucles réseau et pour fournir des liaisons de sauvegarde entre les commutateurs, les ponts ou les routeurs. Ceci permet au commutateur d'interagir avec d'autres périphériques-ponts (à savoir un commutateur compatible STA, un pont ou un routeur) dans votre réseau afin de garantir qu'une seule route existe entre deux stations du réseau et de fournir des liaisons de sauvegarde qui remplacent automatiquement les liaisons primaires désactivés.

Exemple

L'exemple suivant active l'algorithme Spanning Tree pour ce commutateur :

```
Console(config)#spanning-tree
Console(config)#
```

4.3.11.2 spanning-tree mode

Cette commande permet de sélectionner le mode Spanning Tree pour ce commutateur. Utilisez la forme **no** pour restaurer la valeur par défaut.

Syntaxe

spanning-tree mode {**stp** | **rstp**}
no spanning-tree mode

- **stp** : Protocole Spanning Tree (IEEE 802.1D)
- **rstp** : Spanning Tree Rapide (IEEE 802.1w)

Configuration par défaut

stp

Mode de commande

Global Configuration

Utilisation de la commande

- Protocole Spanning Tree Rapide

  Le RSTP prend en charge les connexions aux noeuds STP ou RSTP en surveillant les messages de protocole entrants et en modifiant de manière dynamique le type de messages de protocole transmis par le noeud RSTP tel que décrit ci-dessous :

  - Mode STP : Si le commutateur reçoit un BPDU 802.1D après l'expiration du délai de migration d'un port, le commutateur suppose qu'il est connecté à un pont 802.1D et commence à n'utiliser que des BPDU 802.1D.
  - Mode RSTP : Si le RSTP utilise des BPDU 802.1D sur un port et reçoit un BPDU RSTP après l'expiration du délai de migration, le RSTP réinitialise l'horloge de migration et commence à utiliser des BPDU RSTP sur ce port.

Exemple

L'exemple suivant configure le commutateur afin qu'il utilise le Spanning Tree Rapide :

```
Console(config)#spanning-tree mode rstp
Console(config)#
```

4.3.11.3 spanning-tree forward-time

Cette commande permet de configurer le délai de transmission du pont Spanning Tree globalement pour ce commutateur. Utilisez la forme **no** pour restaurer la valeur par défaut.

Syntaxe

spanning-tree forward-time *seconds*
no spanning-tree forward-time

seconds : Délai en secondes. (Plage : 4-30 secondes)
La valeur minimale est la plus élevée de 4 ou [(max-age / 2) + 1].

Configuration par défaut

15 secondes

Mode de commande

Global Configuration

Utilisation de la commande

Cette commande définit le délai maximal (en secondes) d'attente du périphérique racine avant un changement d'état (ignorer - apprendre - transmettre). Ce délai est nécessaire pour que chaque périphérique puisse recevoir des informations sur les changements de topologie avant de commencer à transmettre les trames. En outre, chaque port a besoin de temps pour écouter les informations conflictuelles qui le renverraient à l'état « ignorer », sans quoi des boucles de données temporaires pourraient apparaître.

Exemple

```
Console(config)#spanning-tree forward-time 20
Console(config)#
```

4.3.11.4 spanning-tree hello-time

Cette commande permet de configurer le délai de connexion du pont Spanning Tree globalement pour ce commutateur. Utilisez la forme **no** pour restaurer la valeur par défaut.

Syntaxe

spanning-tree hello-time *time*
no spanning-tree hello-time

time : Délai en secondes. (Plage : 1-10 secondes)
La valeur maximale est la plus basse de 10 ou [(max-age / 2) -1].

Configuration par défaut

2 secondes

Mode de commande

Global Configuration

Utilisation de la commande

Cette commande définit l'intervalle (en secondes) auquel le périphérique racine transmet un message de configuration.

Exemple

```
Console(config)#spanning-tree hello-time 5
Console(config)#
```

4.3.11.5 spanning-tree max-age

Cette commande permet de configurer l'âge maximal du pont Spanning Tree globalement pour ce commutateur. Utilisez la forme **no** pour restaurer la valeur par défaut.

Syntaxe

spanning-tree max-age *seconds*
no spanning-tree max-age

seconds : Délai en secondes. (Plage : 6-40 secondes)
La valeur minimale est la plus élevée de 6 ou [2 x (hello-time + 1)].
La valeur maximale est la plus basse de 40 ou [2 x (forward-time -1)].

Configuration par défaut

20 secondes

Mode de commande

Global Configuration

Utilisation de la commande

Cette commande définit le délai maximal (en secondes) d'attente d'un périphérique qui ne reçoit pas de messages de configuration avant qu'il tente une reconfiguration. Tous les ports de périphériques (à l'exception des ports désignés) doivent recevoir des messages de configuration à intervalle régulier. Le port qui élimine les informations STA (fournies dans le dernier message de configuration reçu) pour cause d'obsolescence devient le port désigné pour le LAN connecté. S'il s'agit d'un port racine, un nouveau port racine est sélectionné parmi les ports de périphériques connectés au réseau.

Exemple

```
Console(config)#spanning-tree max-age 40
Console(config)#
```

4.3.11.6 spanning-tree priority

Cette commande permet de configurer la priorité du Spanning Tree globalement pour ce commutateur. Utilisez la forme **no** pour restaurer la valeur par défaut.

Syntaxe

spanning-tree priority *priority*
no spanning-tree priority

priority : Priorité du pont.
(Plage : 0-61440, par incréments de 4096 ; Options : 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440)

Configuration par défaut

32768

Mode de commande

Global Configuration

Utilisation de la commande

La priorité du pont sert à sélectionner le périphérique racine, le port racine et le port désigné. Le périphérique avec la priorité la plus élevée devient le périphérique racine du STA. Toutefois, si tous les périphériques ont la même priorité, le périphérique racine est celui avec l'adresse MAC la moins élevée.

Exemple

```
Console(config)#spanning-tree priority 40000
Console(config)#
```

4.3.11.7 spanning-tree pathcost method

Cette commande permet de configurer la méthode de détermination de la distance parcourue pour le Spanning Tree Rapide. Utilisez la forme **no** pour restaurer la valeur par défaut.

Syntaxe

spanning-tree pathcost method {**long** | **short**}
no spanning-tree pathcost method

- **long** : Spécifie les valeurs basées sur 32 bits situées dans une plage de 1 à 200 000 000.
- **short** : Spécifie les valeurs basées sur 16 bits situées dans une plage de 1 à 65535.

Configuration par défaut

Méthode « short »

Mode de commande

Global Configuration

Utilisation de la commande

La méthode de détermination de la distance parcourue sert à déterminer le meilleur chemin entre deux périphériques. C'est pourquoi les valeurs inférieures doivent être affectées aux ports attachés aux supports les plus rapides, et les valeurs supérieures aux ports avec les supports les plus lents. Remarquez que la distance parcourue (page 4-99) est prioritaire sur le port (page 4-100).

Exemple

```
Console(config)#spanning-tree pathcost method long
Console(config)#
```

4.3.11.8 spanning-tree transmission-limit

Cette commande permet de configurer l'intervalle minimal entre la transmission de BPDU RSTP consécutifs. Utilisez la forme **no** pour restaurer la valeur par défaut.

Syntaxe

spanning-tree transmission-limit *count*
no spanning-tree transmission-limit

count : Limite de transmission en secondes. (Plage : 1-10)

Configuration par défaut

3

Mode de commande

Global Configuration

Utilisation de la commande

Cette commande limite le taux de transmission maximal pour les BPDU.

Exemple

```
Console(config)#spanning-tree transmission-limit 4
Console(config)#
```

4.3.11.9 spanning-tree cost

Cette commande permet de configurer la distance à parcourir du Spanning Tree pour l'interface spécifiée. Utilisez la forme **no** pour restaurer la valeur par défaut.

Syntaxe

spanning-tree cost *cost*
no spanning-tree cost

cost : Distance à parcourir pour l'interface.
(Plage : 1-200 000 000)
La plage recommandée est :

- Ethernet : 200 000-20 000 000
- Fast Ethernet : 20 000-2 000 000
- Gigabit Ethernet : 2 000-200 000

Configuration par défaut

- Ethernet : semi-duplex : 2 000 000 ; duplex : 1 000 000 ; groupe : 500 000
- Fast Ethernet : semi duplex : 200 000 ; duplex : 100 000 ; groupe : 50 000
- Gigabit Ethernet : duplex : 10 000 ; groupe : 5 000

Mode de commande

Interface Configuration (Ethernet, Port Channel)

Utilisation de la commande

- Cette commande est utilisée par l'algorithme Spanning Tree pour déterminer la distance à parcourir entre les deux périphériques. C'est pourquoi les valeurs inférieures doivent être affectées aux interfaces attachées aux supports les plus rapides, et les valeurs supérieures aux interfaces avec les supports les plus lents.
- La distance à parcourir passe avant la priorité de l'interface.
- Lorsque la méthode de détermination de la distance à parcourir est « short », la valeur maximale de la distance à parcourir est de 65 535.

Exemple

```
Console(config)#interface ethernet SNP5
Console(config-if)#spanning-tree cost 50
Console(config-if)#
```

Commandes associées

spanning-tree port-priority (4-100)

4.3.11.10 spanning-tree port-priority

Cette commande permet de configurer la priorité de l'interface spécifiée. Utilisez la forme **no** pour restaurer la valeur par défaut.

Syntaxe

spanning-tree port-priority *priority*
no spanning-tree port-priority

priority : Priorité d'une interface. (Plage : 0-240, par incréments de 16)

Configuration par défaut

128

Mode de commande

Interface Configuration (Ethernet, Port Channel)

Utilisation de la commande

- Cette commande définit la priorité pour l'utilisation d'une interface dans l'algorithme Spanning Tree. Si la distance à parcourir pour toutes les interfaces d'un commutateur est identique, l'interface avec la priorité la plus élevée (à savoir la valeur la plus basse) sera configurée comme liaison active dans le Spanning Tree.
- Si plusieurs interfaces possèdent la priorité la plus élevée, le port avec l'identificateur numérique le plus bas sera activé.

Exemple

```
Console(config)#interface ethernet SNP5
Console(config-if)#spanning-tree port-priority 0
Console(config-if)#
```

Commandes associées

spanning-tree cost (4-99)

4.3.11.11 spanning-tree edge-port

Cette commande permet de spécifier une interface comme port de périphérie. Utilisez la forme **no** pour restaurer la valeur par défaut.

Syntaxe

spanning-tree edge-port
no spanning-tree edge-port

Configuration par défaut

NETP0-7, NETMGT: désactivés
SNP0-15 : activé (valeur fixe)

Mode de commande

Interface Configuration (Ethernet, Port Channel)

Utilisation de la commande

Vous pouvez activer cette option si une interface est attachée à un segment LAN qui se trouve à la fin d'un LAN ponté ou sur un noeud terminal. Etant donné que les noeuds finaux ne peuvent pas provoquer de boucles de transmission, ils peuvent passer directement à l'état de transmission du Spanning Tree. Spécifier les ports de périphérie permet une convergence plus rapide pour les périphériques tels que les stations de travail ou les serveurs, conserve la base de données de transmission courante pour réduire la quantité de trames envoyées requise pour régénérer les tables d'adressage pendant les événements de reconfiguration, n'induit pas de reconfiguration lorsque l'interface change d'état et permet également de gérer d'autres problèmes de temporisation liés au STA. Toutefois, rappelez-vous que le port de périphérie ne doit être activé que pour les ports connectés à un périphérique de noeud final.

Exemple

```
Console(config)#interface ethernet SNP5
Console(config-if)#spanning-tree edge-port
Console(config-if)#
```

4.3.11.12 spanning-tree protocol-migration

Cette commande permet de réactiver le format approprié pour les BPDU à envoyer sur l'interface sélectionnée.

Syntaxe

spanning-tree protocol-migration *interface*

interface

- **ethernet** *port-name*
  port-name : liaison descendante : SNP0-15 ; liaison ascendante : NETP0-7 ; gestion : NETMGT
- **port-channel** *channel-id* (Plage : 1-6)

Mode de commande

Privileged Exec

Utilisation de la commande

Si, à un moment donné, le commutateur détecte des BPDU STP, y compris des BDPU Configuration ou Topology Change Notification, il définit automatiquement l'interface sélectionnée au mode compatibilité STP forcée. Toutefois, vous pouvez également utiliser la commande **spanning-tree protocol-migration** à tout moment pour réactiver manuellement le format approprié (compatible RSTP ou STP) pour les BPDU à envoyer sur les interfaces sélectionnées.

Exemple

```
Console(config)#interface ethernet SNP5
Console(config-if)#spanning-tree protocol-migration
Console(config-if)#
```

4.3.11.13 spanning-tree link-type

Cette commande permet de configurer le type de liaison pour le Spanning Tree Rapide. Utilisez la forme **no** pour restaurer la valeur par défaut.

Syntaxe

spanning-tree link-type {**auto** | **point-to-point** | **shared**}
no spanning-tree link-type

- **auto** : Dérivé automatiquement du paramètre du mode duplex.
- **point-to-point** : Liaison point-par-point.
- **shared** : Support partagé.

Configuration par défaut

auto

Mode de commande

Interface Configuration (Ethernet, Port Channel)

Utilisation de la commande

- Spécifiez une liaison point-par-point si l'interface ne peut être connectée qu'à un seul autre pont, ou une liaison partagée si elle peut être connectée à deux ou plusieurs ponts.
- Lorsque la détection automatique est sélectionnée, le commutateur dérive le type de liaison du mode duplex. Une interface duplex est considérée comme liaison point-par-point, alors qu'une interface en semi duplex est supposée être une liaison partagée.
- RSTP ne fonctionne que sur des liaisons point-par-point entre deux ponts. Si vous désignez un port comme liaison partagée, l'utilisation du RSTP est impossible.

Exemple

```
Console(config)#interface ethernet SNP5
Console(config-if)#spanning-tree link-type point-to-point
Console(config-if)#
```

4.3.11.14 show spanning-tree

Cette commande permet d'afficher la configuration du Spanning Tree.

Syntaxe

show spanning-tree [*interface*]

- *interface*
  - **ethernet** *port-name*
    port-name : liaison descendante : SNP0-15 ; liaison ascendante : NETP0-7 ; gestion : NETMGT
  - **port-channel** *channel-id* (Plage : 1-6)

Configuration par défaut

Aucune

Mode de commande

Privileged Exec

Utilisation de la commande

- Utilisez la commande **show spanning-tree** sans paramètres pour afficher la configuration du Spanning Tree du commutateur et de toutes les interface du Spanning Tree.
- Utilisez la commande **show spanning-tree** *interface* pour afficher la configuration du Spanning Tree pour une interface spécifique.
- Pour une description des éléments affichés sous « Informations du groupe de ponts », consultez « Configuration des paramètres STA de base » à la page 3-57. Pour une description des éléments affichés par cette commande, reportez-vous à « Gestion des interfaces pour l'algorithme Spanning Tree » à la page 3-103.

Exemple

```
Console#show spanning-tree
Bridge-group information
------------------------------------------------------
 Spanning tree mode               :RSTP
 Spanning tree enable/disable     :enable
 Priority                         :32768
 Bridge Hello Time (sec.)         :2
 Bridge Max Age (sec.)            :20
 Bridge Forward Delay (sec.)      :15
 Root Hello Time (sec.)           :2
 Root Max Age (sec.)              :20
 Root Forward Delay (sec.)        :15
 Designated Root                  :8.0000E8666672
 Current root port                :0
 Current root cost                :0
 Number of topology changes       :0
 Last topology changes time (sec.):1363
 Transmission limit               :3
 Path Cost Method                 :21
------------------------------------------------------
SNP0 information
------------------------------------------------------
 Admin status         : enable
 Role                 : designate
 State                : forwarding
 Path cost            : 10000
 Priority             : 128
 Designated cost      : 0
 Designated port      : 8.1
 Designated root      : 8.0000E8666672
 Designated bridge    : 8.0000E8666672
 Forward transitions  : 0
 Admin edge port      : disable
 Oper edge port       : disable
 Admin Link type      : point-to-point
 Oper Link type       : point-to-point
.
.
.
Console#
```

4.3.12 Commandes VLAN

Un VLAN représente un groupe de ports qui peuvent se situer n'importe où sur le réseau, mais communiquent comme s'ils appartenaient au même segment physique. Cette section décrit les commandes utilisées pour créer des groupes de VLAN, ajouter des ports membres, spécifier l'utilisateur du marquage VLAN et activer l'enregistrement automatique du VLAN pour l'interface sélectionnée.

Commande	Fonction	Mode	Page
Edition des groupes de VLAN			
vlan database	Passe en mode de base données VLAN pour ajouter, modifier et supprimer des VLAN	GC	4-106
vlan	Configure un VLAN, y compris son identificateur, son nom et son état.	VC	4-106
Configuration d'interfaces VLAN			
interface vlan	Passe en mode de configuration d'interface pour un VLAN spécifié	GC	4-107
switchport mode	Configure le mode d'appartenance au VLAN pour une interface	IC	4-108
switchport acceptable-frame-types	Configure les types de trames que doit accepter une interface	IC	4-109
swicthport ingress-filtering	Active le filtrage à l'entrée sur une interface	IC	4-110
switchport native vlan	Configure le PVID (VLAN naturel) d'une interface	IC	4-111
switchport allowed vlan	Configure les VLAN associés à une interface	IC	4-112
switchport gvrp	Active le GVRP pour une interface	IC	4-115
switchport forbidden vlan	Configure les VLAN interdits pour une interface	IC	4-113
Affichage des informations sur les VLAN			
show vlan	Affiche des informations sur le VLAN	NE, PE	4-114
show interfaces status vlan	Affiche l'état de l'interface VLAN spécifiée	NE, PE	4-83
show interfaces switchport	Affiche l'état administratif et opérationnel d'une interface	NE, PE	4-85

4.3.12.1 vlan database

Cette commande permet de passer en mode de base de données VLAN. Toutes les commandes de ce mode sont immédiatement activées.

Configuration par défaut

Aucune

Mode de commande

Global Configuration

Utilisation de la commande

- Utilisez le mode de commande de la base de données VLAN pour ajouter, modifier ou supprimer des VLAN. Une fois les modifications de configuration apportées, vous pouvez afficher les paramètres VLAN en entrant la commande **show vlan**.
- Utilisez le mode de commande **interface vlan** pour définir le mode d'appartenance du port et pour ajouter ou supprimer des ports d'un VLAN. Les résultats de ces commandes sont inscrits dans le fichier running-configuration, que vous pouvez consulter en entrant la commande **show running-config**.

Exemple

```
Console(config)#vlan database
Console(config-vlan)#
```

Commandes associées

show vlan (4-114)

4.3.12.2 vlan

Cette commande permet de configurer un VLAN. Utilisez la forme **no** pour restaurer les paramètres par défaut ou supprimer un VLAN.

Syntaxe

vlan *vlan-id* [**name** *vlan-name*] **media ethernet** [**state** {**active** | **suspend**}]
no vlan *vlan-id* [**name** | **state**]

- *vlan-id* : Identificateur du VLAN configuré. (Plage : 1-4094, aucun zéro à l'initiale)
- **name** : Mot-clé devant être suivi par le nom du VLAN.
  - vlan-name : Chaîne ASCII de 1 à 15 caractères.
- **media ethernet** : Type de support Ethernet.
- **state** : Mot-clé devant être suivi par l'état du VLAN.
  - **active** : Le VLAN est opérationnel.
  - **suspend** : Le VLAN est suspendu. Les VLAN suspendus ne transmettent pas de paquets.

Configuration par défaut

Par défaut, seul le VLAN 1 existe et est actif.

Mode de commande

VLAN Database Configuration

Utilisation de la commande

- **no vlan** *vlan-id* supprime le VLAN.
- **no vlan** *vlan-id* **name** supprime le nom du VLAN.
- **no vlan** *vlan-id* **state** restaure l'état par défaut du VLAN (donc actif).
- Le VLAN 1 ne peut pas être suspendu, mais tous les autres le sont.
- Vous pouvez configurer jusqu'à 255 VLAN sur le commutateur.

Exemple

L'exemple suivant ajoute un VLAN, avec l'identificateur 105 et le nom RD5. Le VLAN est activé par défaut.

```
Console(config)#vlan database
Console(config-vlan)#vlan 105 name RD5 media ethernet
Console(config-vlan)#
```

Commandes associées

show vlan (4-114)

4.3.12.3 interface vlan

Cette commande permet de passer en mode de configuration d'interface pour les VLAN et de configurer une interface physique.

Syntaxe

interface vlan *vlan-id*

vlan-id : ID du VLAN configuré. (Plage : 1-4094, aucun zéro à l'initiale)

Configuration par défaut

Aucune

Mode de commande

Global Configuration

Exemple

L'exemple suivant montre comment définir le mode de configuration d'interface sur VLAN 1, puis affecter une adresse IP au VLAN :

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.254 255.255.255.0
Console(config-if)#
```

Commandes associées

shutdown (4-80)

4.3.12.4 switchport mode

Cette commande permet de configurer le mode d'appartenance du VLAN pour un port. Utilisez la forme **no** pour restaurer la valeur par défaut.

Syntaxe

switchport mode {**trunk** | **hybrid**}
no switchport mode

- **trunk** : Spécifie un port comme point final pour un groupe VLAN. Un groupe représente une liaison directe entre deux commutateurs, de telle sorte que le port transmet des trames marquées qui identifient le VLAN source. Toutefois, remarquez que les trames appartenant au VLAN par défaut du port (associé au PVID) sont envoyées sans balises.
- **hybrid** : Spécifie une interface VLAN hybride. Le port peut transmettre des trames marquées ou non marquées.

Configuration par défaut

Tous les ports sont en mode hybride avec un PVID défini à VLAN 1.

Mode de commande

Interface Configuration (Ethernet, Port Channel)

Exemple

L'exemple suivant montre comment définir la valeur « port SNP1 » pour le mode de configuration, puis « hybrid » pour le mode switchport :

```
Console(config)#interface ethernet SNP1
Console(config-if)#switchport mode hybrid
Console(config-if)#
```

4.3.12.5 switchport acceptable-frame-types

Cette commande permet de configurer les types de trames acceptables pour un port. Utilisez la forme **no** pour restaurer la valeur par défaut.

Syntaxe

switchport acceptable-frame-types {**all** | **tagged**}
no switchport acceptable-frame-types

- **all** : Le port accepte toutes trames, marquées ou non.
- **tagged** : Le port ne reçoit que des trames marquées.

Configuration par défaut

Tous les types de trames

Mode de commande

Interface Configuration (Ethernet, Port Channel)

Utilisation de la commande

Lorsque cette option est définie de sorte à recevoir tous les types de trames, les trames non balisées reçues sont affectées au VLAN par défaut.

Exemple

L'exemple suivant montre comment limiter le trafic reçu sur SNP1 aux trames marquées :

```
Console(config)#interface ethernet SNP1
Console(config-if)#switchport acceptable-frame-types tagged
Console(config-if)#
```

4.3.12.6 switchport ingress-filtering

Cette commande permet d'activer le filtrage à l'entrée pour une interface. Utilisez la forme **no** pour restaurer la valeur par défaut.

Syntaxe

switchport ingress-filtering
no switchport ingress-filtering

Configuration par défaut

Désactivé

Mode de commande

Interface Configuration (Ethernet, Port Channel)

Utilisation de la commande

- Le filtrage à l'entrée n'affecte que les trames marquées.
- Si le filtrage à l'entrée est désactivé, l'interface accepte les trames marquées VLAN si la marque correspond à un VLAN connu du commutateur (sauf dans le cas d'un VLAN explicitement interdit sur ce port).
- Si le filtrage à l'entrée est activé, l'interface ignore les trames entrantes marquées pour des VLAN qui ne comptent pas ce port d'entrée parmi leurs membres.
- Le filtrage à l'entrée n'affecte pas les trames BPDU indépendantes du VLAN, telles que GVRP ou STP. Toutefois, il affecte les trames BPDU dépendantes du VLAN, telles que GMRP.

Exemple

L'exemple suivant montre comment définir la valeur « port SNP1 » pour l'interface, puis activer le filtrage à l'entrée :

```
Console(config)#interface ethernet SNP1
Console(config-if)#switchport ingress-filtering
Console(config-if)#
```

4.3.12.7 switchport native vlan

Cette commande permet de configurer le PVID (le VID par défaut) pour une interface. Utilisez la forme **no** pour restaurer la valeur par défaut.

Syntaxe

switchport native vlan *vlan-id*
no switchport native vlan

vlan-id : Identificateur du VLAN par défaut pour une interface. (Plage : 1-4094, aucun zéro à l'initiale)

Configuration par défaut

VLAN 1

Mode de commande

Interface Configuration (Ethernet, Port Channel)

Utilisation de la commande

- Si une interface n'est pas membre du VLAN 1 et si vous affectez son PVID à ce VLAN, l'interface sera ajoutée automatiquement au VLAN 1 sous la forme d'un membre non marqué. Pour tous les autres VLAN, il convient de d'abord configurer une interface sous la forme d'un membre non marqué avant de pouvoir affecter son PVID à ce groupe.
- Si la valeur des types de trames acceptables est **all** ou si le mode switchport est défini à **hybrid**, le PVID est inséré dans toutes les trames non marquées pénétrant sur le port d'entrée.

Exemple

L'exemple suivant montre comment donner au PVID du port SNP1 la valeur « VLAN 3 » :

```
Console(config)#interface ethernet SNP1
Console(config-if)#switchport native vlan 3
Console(config-if)#
```

4.3.12.8 switchport allowed vlan

Cette commande permet de configurer les groupes de VLAN sur l'interface sélectionnée. Utilisez la forme **no** pour restaurer la valeur par défaut.

Syntaxe

switchport allowed vlan {**add** *vlan* [**tagged** | **untagged**] | **remove** *vlan*}

- **add** *vlan* : Identificateur de VLAN à ajouter.
- **remove** *vlan* : Identificateur de VLAN à supprimer.

  N'entrez pas de zéros à l'initiale. (Gamme : 1-4094)

no switchport allowed vlan

Remarque : Vous ne pouvez pas utiliser la commande **no switchport allowed vlan** sur le port NETMGT. (Si vous le faites, le commutateur affiche un message d'erreur). Pour restaurer le port de gestion à son VLAN usine par défaut (à savoir le VLAN 2) et le supprimer de tous les autres VLAN auxquels vous l'avez ajouté, entrez les commandes suivantes :

```
Console(config)#interface ethernet NETMGT
Console(config-if)#switchport allowed vlan add 2
Console(config-if)#switchport native vlan 2
Console(config-if)#switchport allowed vlan remove <vlan id>
```

où *<vlan id>* représente le numéro du VLAN autre que le VLAN 2 auquel vous avez ajouté NETMGT. (Répétez la dernière commande pour tous les VLAN autres que le VLAN 2 dont NETMGT est toujours membre).

Configuration par défaut

- Tous les ports (à l'exception de NETMGT) sont affectés au VLAN 1 par défaut. NETMGT est affecté au VLAN 2 par défaut.
- Le type de trame par défaut est non marqué.

Mode de commande

Interface Configuration (Ethernet, Port Channel)

Utilisation de la commande

- Si la valeur du mode switchport est **trunk**, vous ne pouvez affecter une interface aux groupes de VLAN qu'en tant que membre marqué.
- Les trames sont toujours marquées au sein du commutateur. Le paramètre marqué/non marqué utilisé lorsque vous ajoutez un VLAN à une interface indique au commutateur s'il doit conserver ou supprimer le marquage d'une trame à la sortie.

- Si les VLAN ne sont pris en charge par aucun des périphériques réseau intermédiaires ni par l'hôte situé à l'autre extrémité, l'interface doit être ajoutée à ces VLAN sous la forme d'un membre non marqué. Dans le cas contraire, il suffit d'ajouter au plus un VLAN non marqué, et celui-ci doit correspondre au VLAN naturel de l'interface.
- Si un VLAN figurant dans la liste interdite d'une interface est ajouté manuellement à celle-ci, le VLAN est automatiquement supprimé de la liste relative à cette interface.

Exemple

L'exemple suivant montre comment ajouter les VLAN 1, 2, 5 et 6 à la liste autorisée en tant que VLAN marqués pour le port SNP1 :

```
Console(config)#interface ethernet SNP1
Console(config-if)#switchport allowed vlan add 1 tagged
Console(config-if)#switchport allowed vlan add 2 tagged
Console(config-if)#switchport allowed vlan add 5 tagged
Console(config-if)#switchport allowed vlan add 6 tagged
Console(config-if)#
```

4.3.12.9 switchport forbidden vlan

Cette commande permet de configurer des VLAN interdits. Utilisez la forme **no** pour supprimer la liste des VLAN interdits.

Syntaxe

switchport forbidden vlan {**add** *vlan* | **remove** *vlan*}
no switchport forbidden vlan

- **add** *vlan* : Identificateur du VLAN à ajouter.
- **remove** *vlan* : Identificateur du VLAN à supprimer.

  N'entrez pas de zéros à l'initiale. (Plage : 1-4094)

Configuration par défaut

Aucun VLAN n'est inclus dans la liste interdite.

Mode de commande

Interface Configuration (Ethernet, Port Channel)

Utilisation de la commande

- Cette commande empêche l'ajout automatique d'un VLAN à une interface spécifique par le biais du GVRP.
- Si un VLAN a été ajouté aux VLAN autorisés pour une interface, vous ne pouvez pas l'ajouter aux VLAN interdits pour cette même interface.

Exemple

L'exemple suivant montre comment empêcher l'ajout du port SNP1 au VLAN 3 :

```
Console(config)#interface ethernet SNP1
Console(config-if)#switchport forbidden vlan add 3
Console(config-if)#
```

4.3.12.10 show vlan

Cette commande permet d'afficher des informations sur les VLAN.

Syntaxe

show vlan [**id** *vlan-id* | **name** *vlan-name*]

- **id** : Mot-clé devant être suivi par l'identificateur du VLAN.
  - *vlan-id* : Identificateur du VLAN configuré. (Plage : 1-4094, aucun zéro à l'initiale)
- **name** : Mot-clé devant être suivi par le nom du VLAN.
  - *vlan-name* : Chaîne ASCII de 1 à 15 caractères.

Configuration par défaut

Affiche tous les VLAN

Mode de commande

Normal Exec, Privileged Exec

Exemple

L'exemple suivant montre comment afficher des informations sur le VLAN 1 :

```
Console#show vlan id 1
VLAN Type    Name             Status    Ports/Channel groups
---- ------- ---------------- --------- ---------------------------------------
   1  Static      DefaultVlan   Active   SNP0    SNP1    SNP2    SNP3    SNP4
                                           SNP5    SNP6    SNP7    SNP8    SNP9
                                          SNP10   SNP11   SNP12   SNP13   SNP14
                                          SNP15   NETP0   NETP1   NETP2   NETP3
                                          NETP4   NETP5   NETP6   NETP7
   2  Static          MgtVlan    Active  NETMGT
Console#
```

4.3.13 Commandes GVRP et Bridge Extension

Le protocole GVRP (GARP VLAN Registration Protocol) définit une méthode permettant aux commutateurs d'échanger des informations sur le VLAN afin d'enregistrer automatiquement les membres des VLAN sur les interfaces du réseau. Cette section décrit la procédure permettant d'activer le GVRP pour des interfaces individuelles et globalement pour le commutateur, ainsi que la marche à suivre pour afficher les paramètres de configuration par défaut de la MIB Bridge Extension.

Commande	Fonction	Mode	Page
Commandes d'interface			
switchport gvrp	Active le GVRP pour une interface	IC	4-115
switchport forbidden vlan	Configure les VLAN interdits pour une interface	IC	4-113
show gvrp configuration	Affiche la configuration GVRP pour l'interface sélectionnée	NE, PE	4-116
garp timer	Définit l'horloge GARP pour la fonction sélectionnée	IC	4-117
show garp timer	Affiche l'horloge GARP pour la fonction sélectionnée	NE, PE	4-118
Commandes globales			
bridge-ext gvrp	Active le GVRP globalement pour le commutateur	GC	4-119
show bridge-ext	Affiche la configuration « Bridge Extension » (extension du pont)	PE	4-120

4.3.13.1 switchport gvrp

Cette commande permet d'activer le GVRP pour un port. Utilisez la forme **no** pour désactiver cette fonction.

Syntaxe

switchport gvrp
no switchport gvrp

Configuration par défaut

Activé

Mode de commande

Interface Configuration (Ethernet, Port Channel)

Exemple

```
Console(config)#interface ethernet SNP1
Console(config-if)#switchport gvrp
Console(config-if)#
```

4.3.13.2 show gvrp configuration

Cette commande permet d'afficher l'activation/la désactivation du GVRP.

Syntaxe

show gvrp configuration [*interface*]

interface

- **ethernet** *port-name*
  port-name : liaison descendante : SNP0-15 ; liaison ascendante : NETP0-7 ; gestion : NETMGT
- **port-channel** *channel-id* (Plage : 1-6)

Configuration par défaut

Affiche la configuration globale ainsi que la configuration spécifique à l'interface.

Mode de commande

Normal Exec, Privileged Exec

Exemple

```
Console#show gvrp configuration
Whole system:
GVRP configuration: Enabled
SNP0:
 Gvrp configuration: Enabled
SNP1:
 Gvrp configuration: Enabled
.
.
.
```

4.3.13.3 garp timer

Cette commande permet de définir les valeurs des horloges join, leave et leaveall. Utilisez la forme **no** pour restaurer les valeurs par défaut des horloges.

Syntaxe

garp timer {**join** | **leave** | **leaveall**} *timer_value*
no garp timer {**join** | **leave** | **leaveall**}

- {**join** | **leave** | **leaveall**} : Horloge à configurer.
- *timer_value* : Valeur de l'horloge.
  Plage :
  - join : 20-1000 centisecondes
  - leave : 60-3000 centisecondes
  - leaveall : 500-18000 centisecondes

Configuration par défaut

- join : 20 centisecondes
- leave : 60 centisecondes
- leaveall : 1000 centisecondes

Mode de commande

Interface Configuration (Ethernet, Port Channel)

Utilisation de la commande

- Le protocole GARP (Group Address Registration Protocol) est utilisé par les protocoles GVRP et GMRP pour enregistrer ou désenregistrer les attributs du client pour les services clients dans un LAN muni de ponts. Les valeurs par défaut des horloges GARP sont indépendantes de la méthode d'accès aux supports ou des taux de données. Ces valeurs ne doivent pas être modifiées à moins que vous rencontriez des difficultés avec l'enregistrement/le désenregistrement GVRP ou GMRP.
- Les valeurs des horloges sont appliquées au GVRP pour tous les ports de tous les VLAN.
- Les valeurs des horloges respectent les restrictions suivantes :
  - leave >= (2 x join)
  - leaveall > leave

Remarque - Définissez les mêmes valeurs pour les horloges GVRP sur tous les périphériques de la couche 2 connectés au même réseau. Sinon, le GVRP ne fonctionnera pas correctement.

Exemple

```
Console(config)#interface ethernet SNP1
Console(config-if)#garp timer join 100
Console(config-if)#
```

Commandes associées

show garp timer (4-118)

4.3.13.4 show garp timer

Cette commande permet d'afficher les horloges GARP pour l'interface sélectionnée.

Syntaxe

show garp timer [*interface*]

interface

- **ethernet** *port-name*
  port-name : liaison descendante : SNP0-15 ; liaison ascendante : NETP0-7 ; gestion : NETMGT
- **port-channel** *channel-id* (Plage : 1-6)

Configuration par défaut

Affiche toutes les horloges GARP.

Mode de commande

Normal Exec, Privileged Exec

Exemple

```
Console#show garp timer ethernet SNP1
SNP1 GARP timer status:
 Join timer: 20 sec.
 Leave timer: 60 sec.
 Leaveall timer: 1000 sec.
Console#
```

Commandes associées

garp timer (4-117)

4.3.13.5 bridge-ext gvrp

Cette commande permet d'activer le GVRP globalement pour ce commutateur. Utilisez la forme **no** pour désactiver cette fonction.

Syntaxe

bridge-ext gvrp
no bridge-ext gvrp

Configuration par défaut

Enabled

Mode de commande

Global Configuration

Utilisation de la commande

Le protocole GVRP définit une méthode permettant aux commutateurs d'échanger des informations sur les VLAN afin d'enregistrer les membres des VLAN sur tous les ports du réseau. Cette fonction doit être activée pour permettre un enregistrement automatique des VLAN et pour prendre en charge les VLAN sortant du cadre du commutateur local.

Exemple

```
Console(config)#bridge-ext gvrp
Console(config)#
```

4.3.13.6 show bridge-ext

Cette commande permet d'afficher la configuration des commandes Bridge Extension.

Configuration par défaut

Aucune

Mode de commande

Privileged Exec

Utilisation de la commande

La signification des éléments affichés par cette commande est la suivante :

- **Max support vlan numbers** : Version du VLAN utilisée par ce commutateur telle que spécifiée dans la norme IEEE 802.1Q.
- **Max support vlan ID** : Identificateur du VLAN max. reconnue par ce commutateur.
- **Extended multicast filtering services** : Le commutateur ne prend pas en charge le filtrage des adresses multidestinataires sur la base du protocole GMRP (GARP Multicast Registration Protocol).
- **Static entry individual port** : Le commutateur prend en charge le filtrage statique des adresses unidestinataires et multidestinataires (page 4-87 et 4-123).
- **VLAN learning** : Le commutateur utilise l'IVL (Independant VLAN Learning) où chaque port gère sa propre base de données de filtrage.
- **Configurable PVID tagging** : Le commutateur vous permet d'ignorer l'identificateur du VLAN du port par défaut (PVID utilisé dans les marques de trames) et l'état de sortie (marqués ou non marqués VLAN) sur chaque port (page 4-111).
- **Local VLAN capable** : Cet élément se rapporte à la prise en charge par le commutateur du Spanning Tree Multiple. Actuellement, le Spanning Tree Multiple n'est pas pris en charge.
- **Traffic classes** : Le commutateur permet l'affectation des priorités utilisateur à plusieurs classes de trafic (page 4-135).
- **Global GVRP status** : Le protocole GVRP (GARP VLAN Registration Protocol) définit une méthode permettant aux commutateurs d'échanger des informations sur les VLAN afin d'enregistrer les membres des VLAN nécessaires sur tous les ports du réseau. Cette fonction doit être activée pour la prise en charge des groupes de VLAN dépassant le commutateur local (page 4-119).
- **GMRP** : Le protocole GMRP (GARP Multicast Registration Protocol) permet aux périphériques réseau d'enregistrer les stations terminales auprès des groupes multidestinataires. Ce commutateur ne prend pas le protocole GMRP en charge ; il utilise le protocole IGMP (Internet Group Management Protocole) pour assurer le filtrage multidestinataire automatique.

Exemple

```
Console#show bridge-ext
 Max support vlan numbers: 255
 Max support vlan ID: 4094
 Extended multicast filtering services: No
 Static entry individual port: Yes
 VLAN learning: IVL
 Configurable PVID tagging: Yes
 Local VLAN capable: Yes
 Traffic classes: Enabled
 Global GVRP status: Enabled
 GMRP: Disabled
Console#
```

4.3.14 Commandes de l'IGMP Snooping

Ce commutateur utilise le protocole IGMP (Internet Group Management Protocol) pour rechercher tous les hôtes attachés qui souhaitent recevoir un service multidestinataire spécifique. Il identifie les ports contenant des hôtes demandant un service et n'envoie des données qu'à ces ports. Ensuite, il propage la requête de service aux commutateurs/routeurs multidestinataires avoisinants afin de s'assurer qu'il continuera à recevoir le service multidestinataire.

Commande	Fonction	Mode	Page
Commandes IGMP de base			
ip igmp snooping	Active l'IGMP Snooping	GC	4-122
ip igmp snooping vlan static	Ajoute une interface à un groupe multidestinataire	GC	4-123
ip igmp snooping version	Configure la version IGMP pour l'IGMP Snooping	GC	4-123
show ip igmp snooping	Affiche la configuration de l'IGMP snooping	PE	4-124
show bridge multicast	Affiche la liste multidestinataire MAC de l'IGMP snooping	PE	4-125
Commandes du requêteur IGMP			
ip igmp snooping querier	Permet à ce périphérique de fonctionner comme requêteur pour l'IGMP Snooping	GC	4-125
ip igmp snooping query-count	Configure le compteur de requêtes	GC	4-126

Commande	Fonction	Mode	Page
ip igmp snooping query-interval	Configure l'intervalle des requêtes	GC	4-127
ip igmp snooping query-max-response-time	Configure le délai de notification	GC	4-128
ip igmp snooping router-port-expire-time	Configure la temporisation des requêtes	GC	4-129
show ip igmp snooping	Affiche la configuration de l'IGMP snooping	PE	4-124
Commandes des routeurs multidestinataires			
ip igmp snooping vlan mrouter	Ajoute un port de routeur multidestinataire	GC	4-130
show ip igmp snooping mrouter	Affiche les ports de routeurs multidestinataires	PE	4-131

4.3.14.1 ip igmp snooping

Cette commande permet d'activer l'IGMP Snooping sur ce commutateur. Utilisez la forme **no** pour désactiver cette fonction.

Syntaxe

ip igmp snooping
no ip igmp snooping

Configuration par défaut

Désactivé

Mode de commande

Global Configuration

Exemple

L'exemple suivant active l'IGMP Snooping

```
Console(config)#ip igmp snooping
Console(config)#
```

4.3.14.2 ip igmp snooping vlan static

Cette commande permet d'ajouter un port à un groupe multidestinataire. Utilisez la forme **no** pour supprimer le port.

Syntaxe

ip igmp snooping vlan *vlan-id* **static** *ip-address interface*
no ip igmp snooping vlan vlan-id static *ip-address interface*

- *vlan-id* : Identificateur du VLAN (Plage : 1-4094)
- *ip-address* : Adresse IP du groupe multidestinataire
- *interface*
  - **ethernet** *port-name*
    port-name : liaison descendante : SNP0-15 ; liaison ascendante : NETP0-7 ; gestion : NETMGT
  - **port-channel** *channel-id* (Plage : 1-6)

Configuration par défaut

Aucune

Mode de commande

Global Configuration

Exemple

L'exemple suivant montre comment configurer statistiquement un groupe multidestinataire sur un port :

```
Console(config)#ip igmp snooping vlan 1 static 224.0.0.12
ethernet SNP5
Console(config)#
```

4.3.14.3 ip igmp snooping version

Cette commande permet de configurer la version de l'IGMP Snooping. Utilisez la forme **no** pour restaurer la valeur par défaut.

Syntaxe

ip igmp snooping version {**1** | **2**}
no ip igmp snooping version

- **1** : IGMP Version 1
- **2** : IGMP Version 2

Configuration par défaut

IGMP Version 2

Mode de commande

Global Configuration

Utilisation de la commande

- Tous les systèmes du sous-réseau doivent prendre en charge la même version. Si vous disposez de périphériques anciens sur votre réseau et que ceux-ci ne prennent en charge que la version 1, vous devez également configurer le commutateur pour qu'il utilise la version 1.
- Certaines commandes ne sont activées que pour IGMPv2, notamment **ip igmp query-max-response-time** et **ip igmp query-timeout**.

Exemple

L'exemple suivant configure le commutateur afin qu'il utilise la version 1 de l'IGMP :

```
Console(config)#ip igmp snooping version 1
Console(config)#
```

4.3.14.4 show ip igmp snooping

Cette commande permet d'afficher la configuration de l'IGMP Snooping.

Configuration par défaut

Aucune

Mode de commande

Privileged Exec

Utilisation de la commande

Consultez « Configuration des paramètres IGMP Snooping » à la page 3-46 pour une description des éléments affichés.

Exemple

L'exemple suivant affiche la configuration actuelle de l'IGMP Snooping.

```
Console#show ip igmp snooping
 Service status          : Enabled
 Querier status: Enabled
 Query count: 2
 Query interval: 125 sec
 Query max response time: 10 sec
 Query time-out: 300 sec
 IGMP snooping version: Version 2
Console#
```

4.3.14.5 show mac-address-table multicast

Cette commande permet d'afficher les adresses multidestinataires connues.

Syntaxe

show mac-address-table multicast [**vlan** *vlan-id*] [**user** | **igmp-snooping**]

- *vlan-id* : Identificateur du VLAN (1 à 4094)
- **user** : N'affiche que les entrées multidestinataires configurées par l'utilisateur.
- **igmp-snooping** : N'affiche que les entrées apprises par le biais de l'IGMP Snooping.

Configuration par défaut

Aucune

Mode de commande

Privileged Exec

Utilisation de la commande

Les types de membres affichés comprennent IGMP ou USER, selon les options sélectionnées.

Exemple

L'exemple suivant affiche les entrées multidestinataires apprises par le biais de l'IGMP Snooping pour le groupe de ponts 1, VLAN 1 :

```
Console#show mac-address-table multicast vlan 1 igmp-snooping
 VLAN M'cast IP addr. Member ports Type
 ---- --------------- ------------ -------
    1      224.0.0.12        NETP0    USER
    1       224.1.2.3        NETP1    IGMP
Console#
```

4.3.14.6 ip igmp snooping querier

Cette commande permet d'activer le commutateur comme requêteur IGMP Snooping. Utilisez la forme **no** pour désactiver cette fonction.

Syntaxe

ip igmp snooping querier
no ip igmp snooping querier

Configuration par défaut

Désactivée

Mode de commande

Global Configuration

Utilisation de la commande

Si cette fonction est active, le commutateur, s'il est choisi, joue le rôle de requêteur. Le requêteur se charge de demander aux hôtes s'ils souhaitent recevoir le trafic multidestinataire.

Exemple

```
Console(config)#ip igmp snooping querier
Console(config)#
```

4.3.14.7 ip igmp snooping query-count

Cette commande permet de configurer le compteur de requêtes. Utilisez la forme **no** pour restaurer la valeur par défaut.

Syntaxe

ip igmp snooping query-count *count*
no ip igmp snooping query-count

count : Nombre maximum de requêtes émises sans réponse avant que le requêteur n'exclue un client du groupe multidestinataire. (Fourchette : 2-10)

Configuration par défaut

2 fois

Mode de commande

Global Configuration

Utilisation de la commande

Le compteur de requêtes définit le délai pendant lequel le requêteur attend une réponse d'un client multidestinataire avant de réagir. Si un requêteur a envoyé le nombre de requêtes défini par cette commande, mais n'a pas obtenu de réponse du client, une horloge à rebours démarre sur la base du délai défini par **ip igmp snooping query-max-response-time**. Si le compte à rebours se termine sans que le client ait répondu, le système considère que celui-ci a quitté le groupe multidestinataire.

Exemple

L'exemple suivant montre comment configurer le compteur de requêtes à 10 :

```
Console(config)#ip igmp snooping query-count 10
Console(config)#
```

Commandes associées

ip igmp snooping query-max-response-time (4-128)

4.3.14.8 ip igmp snooping query-interval

Cette commande permet de configurer l'intervalle entre les requêtes de l'IGMP Snooping. Utilisez la forme **no** pour restaurer la valeur par défaut.

Syntaxe

ip igmp snooping query-interval *seconds*
no ip igmp snooping query-interval

seconds : Fréquence à laquelle le commutateur envoie des messages host-query IGMP. (Plage : 60-125)

Configuration par défaut

125 secondes

Mode de commande

Global Configuration

Exemple

L'exemple suivant montre comment configurer l'intervalle de requêtes à 100 secondes :

```
Console(config)#ip igmp snooping query-interval 100
Console(config)#
```

4.3.14.9 ip igmp snooping query-max-response-time

Cette commande permet de configurer l'intervalle entre les reports de l'IGMP Snooping. Utilisez la forme **no** pour restaurer la valeur par défaut.

Syntaxe

ip igmp snooping query-max-response-time *seconds*
no ip igmp snooping query-max-response-time

seconds : Délai de notification publié dans les requêtes IGMP. (Plage : 5-25)

Configuration par défaut

10 secondes

Mode de commande

Global Configuration

Utilisation de la commande

- Pour que cette commande soit appliquée, le commutateur doit utiliser IGMPv2.
- Cette commande définit le délai autorisé entre l'envoi d'une requête et la réception d'une réponse du client multidestinataire. Si un requêteur a envoyé le nombre de requêtes défini par **ip igmp snooping query-count**, mais n'a pas obtenu de réponse d'un client, une horloge à rebours démarre sur la base de la valeur initiale définie par cette commande. Si le compte à rebours se termine sans que le client ait répondu, le système considère que celui-ci a quitté le groupe multidestinataire.

Exemple

L'exemple suivant montre comment configurer l'intervalle maximum de requêtes à 20 secondes :

```
Console(config)#ip igmp snooping query-max-response-time 20
Console(config)#
```

Commandes associées

ip igmp snooping version (4-123)
ip igmp snooping query-max-response-time (4-128)

4.3.14.10 ip igmp snooping router-port-expire-time

Cette commande permet de configurer le délai de temporisation des requêtes de l'IGMP Snooping. Utilisez la forme **no** pour restaurer la valeur par défaut.

Syntaxe

ip igmp snooping router-port-expire-time *seconds*
no ip igmp snooping router-port-expire-time

seconds : Délai pendant lequel le commutateur attend, lorsqu'un requêteur arrête d'envoyer des requêtes, avant de considérer que l'interface (qui recevait les paquets de requêtes) n'est plus attachée à un requêteur. (Plage : 300-500)

Configuration par défaut

300 secondes

Mode de commande

Global Configuration

Utilisation de la commande

Pour que cette commande soit appliquée, le commutateur doit utiliser IGMPv2.

Exemple

L'exemple suivant montre comment configurer la temporisation à 500 secondes :

```
Console(config)#ip igmp snooping router-port-expire-time 500
Console(config)#
```

Commandes associées

ip igmp snooping version (4-123)

4.3.14.11 ip igmp snooping vlan mrouter

Cette commande vous permet de configurer un port de routeur multidestinataire de manière statique. Utilisez la forme **no** pour supprimer la configuration.

Syntaxe

ip igmp snooping vlan *vlan-id* **mrouter** *interface*
no ip igmp snooping vlan *vlan-id* **mrouter** *interface*

- *vlan-id* : ID VLAN (Plage : 1-4094)
- *interface*
  - **ethernet** *port-name*
    port-name : liaison descendante : SNP0-15 ; liaison ascendante : NETP0-7 ; gestion : NETMGT
  - **port-channel** *channel-id* (Plage : 1-6)

Configuration par défaut

Aucun port de routeur multidestinataire statique n'est configuré.

Mode de commande

Global Configuration

Utilisation de la commande

Selon vos connexions réseau, l'IGMP snooping peut ne pas toujours être en mesure de localiser le requêteur IGMP. C'est la raison pour laquelle, si le requêteur IGMP est un routeur/commutateur multidestinataire connu connecté par le biais du réseau à une interface (port ou groupe du commutateur), vous pouvez configurer manuellement l'interface afin qu'elle adhère à tous les groupes multidestinataires courants.

Exemple

L'exemple suivant montre comment configurer le port 11 comme port de routage multidestinataire dans le VLAN 1 :

```
Console(config)#ip igmp snooping vlan 1 mrouter ethernet NETP0
Console(config)#
```

4.3.14.12 show ip igmp snooping mrouter

Cette commande vous permet d'afficher des informations sur les ports de routage multidestinataires appris de manière dynamique ou configurés de manière statique.

Syntaxe

show ip igmp snooping mrouter [**vlan** *vlan-id*]

vlan-id : Identificateur du VLAN (Plage : 1-4094)

Configuration par défaut

Affiche les ports de routage multidestinataires pour tous les VLAN configurés.

Mode de commande

Privileged Exec

Utilisation de la commande

Les types de ports de routage multidestinataires affichés comprennent Static ou Dynamic.

Exemple

L'exemple suivant affiche les ports connectés aux routeurs multidestinataires :

```
Console#show ip igmp snooping mrouter
 VLAN M'cast Router Ports Type
 ---- ------------------- -------
    1               NETP5  Static
    2               NETP6  Dynamic
Console#
```

4.3.15 Commandes de priorité

Les commandes décrites dans cette section vous permettent de spécifier les paquets de données prioritaires quand le trafic est placé dans les files d'attente du commutateur en raison de la saturation du réseau. Le commutateur prend en charge la classe de service avec quatre files d'attente correspondants à différentes priorités pour chaque port. Les paquets de données se trouvant dans la file d'attente avec la priorité la plus élevée seront transmis avant ceux de la file d'attente avec la priorité la plus faible. Vous pouvez définir la priorité par défaut de chaque interface, le poids relatif de chaque file d'attente ainsi que l'affectation des marques de priorité des trames aux files d'attente du commutateur.

Commande	Fonction	Mode	Page
Commandes relatives à la priorité de la couche 2			
switchport priority default	Définit une priorité de port pour les trames entrantes non marquées.	IC	4-133
queue bandwidth	Affecte des poids WRR aux files d'attente	GC	4-134
queue cos map	Affecte des valeurs de classe de service aux files d'attente	IC	4-135
show queue bandwidth	Affiche les poids WRR affectés aux files d'attente	PE	4-136
show queue cos-map	Affiche l'affectation des classes de service	PE	4-137
show interfaces switchport	Affiche l'état administratif et opérationnel d'une interface	PE	4-85
Commandes relatives à la priorité des couches 3 et 4			
map ip precedence	Active l'affectation des priorités IP des classes de service	GC	4-137
map ip precedence	Affecte une valeur de priorité IP à une classe de service	IC	4-138
map ip dscp	Active l'affectation DSCP IP des classes de service	GC	4-139
map ip dscp	Affecte une valeur DSCP IP à une classe de service.	IC	4-140
show map ip precedence	Affiche l'affectation des priorités IP	PE	4-141
show map ip dscp	Affiche l'affectation DSCP IP	PE	4-142

4.3.15.1 switchport priority default

Cette commande permet de définir une priorité pour les trames entrantes non marquées ou la priorité des trames reçues par le périphérique connecté à l'interface spécifiée. Utilisez la forme **no** pour restaurer la valeur par défaut.

Syntaxe

switchport priority default *default-priority-id*
no switchport priority default

default-priority-id : numéro de priorité pour le trafic non marqué entrant. La priorité est indiquée un chiffre de 0 à 7, sept étant la priorité la plus élevée.

Configuration par défaut

La priorité n'est pas définie, et la valeur par défaut pour les trames non marquées reçues par l'interface est zéro.

Mode de commande

Configuration de l'interface (Ethernet, canal de port)

Utilisation de la commande

- L'ordre d'affectation des priorités est Priorité IP ou DSCP IP, puis Priorité du port par défaut.
- La priorité par défaut s'applique aux trames non marquées reçues sur un port défini pour accepter tous les types de trames (en d'autres termes, il peut recevoir des trames marquées et non). Cette priorité ne s'applique pas aux trames marquées VLAN IEEE 802.1Q. Si la trame entrante est une trame marquée VLAN IEEE 802.1Q, les bits Priorité utilisateur IEEE 802.1p seront utilisés.
- Ce commutateur propose quatre files d'attente correspondant à différentes priorités sur chaque port. Il est configuré pour utiliser le protocole WRR, ce que vous pouvez voir à l'aide de la commande **queue bandwidth**. Toutes les trames entrantes non marquées par le VLAN reçoivent une marque indiquant la priorité utilisateur par défaut du port d'entrée, puis sont placées dans les files d'attente appropriées sur le port de sortie. La priorité par défaut de tous les ports d'entrée est zéro. C'est la raison pour laquelle toutes les trames entrantes sans marque de priorité sont placées dans la file 0 du port de sortie. (Remarquez que si le port de sortie est un membre non marqué du VLAN associé, toutes les marques VLAN sont supprimées de ces trames avant leur transmission.)

Exemple

L'exemple suivant montre comment définir une priorité par défaut sur les ports SNP3 à 5 :

```
Console(config)#interface ethernet SNP3
Console (config-if)#switchport priority default 5
```

4.3.15.2 queue bandwidth

Cette commande permet d'affecter les poids sur la base du protocole WRR (Weighted Round Robin) pour les quatre files d'attente CdS (Classe de service) avec priorités. Utilisez la forme **no** pour restaurer les poids par défaut.

Syntaxe

queue bandwidth *weight1...weight4*
no queue bandwidth

weight1...weight4 : Le ratio des poids pour les files d'attente 0 à 3 détermine les poids utilisés par le planificateur WRR. (Plage : 1-255)

Configuration par défaut

Les poids 16, 64, 128 et 240 sont affectés à la file d'attente 0, 1, 2 et 3 respectivement.

Mode de commande

Global Configuration

Utilisation de la commande

WRR autorise le partage de la bande passante au port de sortie grâce à la définition des poids de planification.

Exemple

L'exemple suivant montre comment affecter des poids WRR 1, 3, 5 et 7 aux files d'attente CdS 0, 1, 2 et 3 :

```
Console(config)#queue bandwidth 1 3 5 7
Console(config)#
```

Commandes associées

show queue bandwidth (4-136)

4.3.15.3 queue cos-map

Cette commande permet d'affecter des valeurs CdS (Classe de service) aux files d'attente CdS. Utilisez la forme **no** pour définir l'affectation CdS aux valeurs par défaut.

Syntaxe

queue cos-map *queue_id* [*cos1 ... cosn*]
no queue cos-map

- *queue_id* : Identificateur de la file d'attente CdS.
  Les plages sont de 0 à 3, 3 étant la file d'attente CdS avec la priorité la plus élevée.
- *cos1 .. cosn* : Valeurs CdS affectées à l'identificateur de la file d'attente.
  Il s'agit d'une liste de nombres, séparés par des espaces. La valeur CdS est un nombre de 0 à 7, 7 étant la priorité la plus élevée.

Configuration par défaut

Le commutateur prend en charge la classe de service à l'aide de quatre files d'attente pour chaque port, avec une mise en file d'attente WRR (Weighted Round Robin). Huit classes de trafic distinctes sont définies dans IEEE 802.1p. Les niveaux de priorité par défaut sont affectés conformément aux recommandations de la norme IEEE 802.1p, telles que présentées dans le tableau suivant.

	File d'attente			
	0	**1**	**2**	**3**
Priorité		0		
	1			
	2			
		3		
			4	
			5	
				6
				7

Mode de commande

Interface Configuration (Ethernet, Port Channel)

Utilisation de la commande

La CdS affectée au port d'entrée est utilisée pour sélectionner une priorité CdS au port de sortie.

Exemple

L'exemple suivant montre comment affecter les valeurs de CdS 0, 1 et 2 à la file d'attente CdS 0, la valeur 3 à la file d'attente CdS 1, les valeurs 4 et 5 à la file d'attente CdS 2 et les valeurs 6 et 7 à la file d'attente CdS 3.

```
Console(config)#interface ethernet SNP1
Console(config-if)#queue cos-map 0 0 1 2
Console(config-if)#queue cos-map 1 3
Console(config-if)#queue cos-map 2 4 5
Console(config-if)#queue cos-map 3 6 7
Console(config-if)#
```

Commandes associées

show queue cos-map (4-137)

4.3.15.4 show queue bandwidth

Cette commande permet d'afficher l'allocation de la bande passante sur la base du protocole WRR (Weighted Round Robin) pour les quatre files d'attente CdS (Classe de service).

Configuration par défaut

Aucune

Mode de commande

Privileged Exec

Exemple

```
Console#show queue bandwidth
 Queue ID Weight
 -------- ------
    0        16
    1        64
    2        128
    3        240
Console#
```

4.3.15.5 show queue cos-map

Cette commande permet d'afficher l'affectation des priorités CdS.

Syntaxe

show queue cos-map [*interface*]

interface

- **ethernet** *port-name*
  port-name : liaison descendante : SNP0-15 ; liaison ascendante : NETP0-7 ; gestion : NETMGT
- **port-channel** *channel-id* (Plage : 1-6)

Configuration par défaut

Aucune

Mode de commande

Privileged Exec

Exemple

```
Console#show queue cos-map ethernet SNP11
Information of SNP11
 Queue ID Traffic class
 -------- -------------
    0     1 2
    1     0 3
    2     4 5
    3     6 7
Console#
```

4.3.15.6 map ip precedence (Global Configuration)

Cette commande permet d'activer l'affectation de priorités IP (à savoir Type de service IP). Utilisez la forme **no** pour désactiver cette fonction.

Syntaxe

map ip precedence
no map ip precedence

Configuration par défaut

Activée

Mode de commande

Global Configuration

Utilisation de la commande

- L'ordre d'affectation des priorités est Priorité IP ou DSCP IP, puis Priorité du port par défaut.
- Les priorités IP et DSCP IP ne peuvent pas être activées toutes les deux. L'activation de l'un de ces types de priorité désactive automatiquement l'autre.

Exemple

L'exemple suivant montre comment activer l'affectation des priorités IP globalement :

```
Console(config)#map ip precedence
Console(config)#
```

4.3.15.7 map ip precedence (Interface Configuration)

Cette commande permet de définir la priorité IP (à savoir Priorité du Type de service IP). Utilisez la forme **no** pour restaurer la table par défaut.

Syntaxe

map ip precedence *ip-precedence-value* **cos** *cos-value*
no map ip precedence

- *precedence-value* : Valeur de priorité à 3 bits. (Plage : 0-7)
- *cos-value* : Valeur de la classe de service (Plage : 0-7)

Configuration par défaut

Affectation univoque (la valeur de la priorité 0 correspond à la valeur CdS 0, etc.)

Mode de commande

Interface Configuration (Ethernet, Port Channel)

Utilisation de la commande

- L'ordre d'affectation des priorités est Priorité IP ou DSCP IP, puis Priorité du port par défaut.
- Les valeurs de la priorité IP sont affectées aux valeurs CdS par défaut sur une base univoque conformément aux recommandations de la norme IEEE 802.1p, puis aux valeurs par défaut des files d'attente.
- L'affectation de valeurs spécifiques pour la priorité IP est mise en oeuvre comme une commande de configuration d'interface, mais toute modification s'applique à toutes les interfaces du commutateur.

Exemple

L'exemple suivant montre comment affecter la valeur de priorité IP 1 à la valeur CdS 0 :

```
Console(config)#interface ethernet SNP5
Console(config-if)#map ip precedence 1 cos 0
Console(config-if)#
```

4.3.15.8 map ip dscp (Global Configuration)

Cette commande permet d'activer l'affectation IP DSCP (Differentiated Services Code Point). Utilisez la forme **no** pour désactiver l'affectation IP DSCP.

Syntaxe

map ip dscp
no map ip dscp

Configuration par défaut

Activée

Mode de commande

Global Configuration

Utilisation de la commande

- L'ordre d'affectation des priorités est Priorité IP ou DSCP IP, puis Priorité du port par défaut.
- Les priorités IP et DSCP IP ne peuvent pas être activées toutes les deux. L'activation de l'un de ces types de priorité désactive automatiquement l'autre.

Exemple

L'exemple suivant montre comment activer l'affectation IP DSCP globalement :

```
Console(config)#map ip dscp
Console(config)#
```

4.3.15.9 map ip dscp (Interface Configuration)

Cette commande permet de définir la priorité IP DSCP (Differentiated Services Code Point). Utilisez la forme **no** pour restaurer la table par défaut.

Syntaxe

map ip dscp *dscp-value* **cos** *cos-value*
no map ip dscp

- *dscp-value* : Valeur DSCP 8 bits. (Plage : 0-255)
- *cos-value* : Valeur de la classe de service (Plage : 0-7)

Configuration par défaut

Les valeurs DSCP par défaut sont définies dans la table suivante. Remarquez que toutes les valeurs DSCP qui ne sont pas spécifiées sont affectées à la valeur CdS 0.

Valeur IP DSCP	Valeur CdS
0	0
8	1
10, 12, 14, 16	2
18, 20, 22, 24	3
26, 28, 30, 32, 34, 36	4
38, 40, 42	5
48	6
46, 56	7

Mode de commande

Interface Configuration (Ethernet, Port Channel)

Utilisation de la commande

- L'ordre d'affectation des priorités est Priorité IP ou DSCP IP, puis Priorité du port par défaut.
- Les valeurs des priorités DSCP sont affectées aux valeurs CdS par défaut conformément aux recommandations de la norme IEEE 802.1p, puis aux valeurs par défaut des files d'attente.
- L'affectation de valeurs spécifiques pour le DSCP est mise en oeuvre sous la forme d'une commande de configuration d'interface, mais toute modification s'applique à toutes les interfaces du commutateur.

Exemple

L'exemple suivant montre comment affecter la valeur IP DSCP 1 à la valeur CdS 0 :

```
Console(config)#interface ethernet SNP5
Console(config-if)#map ip dscp 1 cos 0
Console(config-if)#
```

4.3.15.10 show map ip precedence

Cette commande permet d'afficher l'affectation des priorités IP Precedence.

Syntaxe

show map ip precedence [*interface*]

interface

- **ethernet** *port-name*
  port-name : liaison descendante : SNP0-15 ; liaison ascendante : NETP0-7 ; gestion : NETMGT
- **port-channel** *channel-id* (Plage : 1-6)

Configuration par défaut

Aucune

Mode de commande

Privileged Exec

Exemple

```
Console#show map ip precedence ethernet SNP5
Precedence mapping status: disabled

 Port         Precedence COS
 -----------  ---------- ---
        SNP5           0   0
        SNP5           1   1
        SNP5           2   2
        SNP5           3   3
        SNP5           4   4
        SNP5           5   5
        SNP5           6   6
        SNP5           7   7
Console#
```

Commandes associées

map ip precedence (Global Configuration) (4-137)
map ip precedence (Interface Configuration) (4-138)

4.3.15.11 show map ip dscp

Cette commande permet d'afficher l'affectation des priorités IP DSCP.

Syntaxe

show map ip dscp [*interface*]

interface

- **ethernet** *port-name*
  port-name : liaison descendante : SNP0-15 ; liaison ascendante : NETP0-7 ; gestion : NETMGT
- **port-channel** *channel-id* (Plage : 1-6)

Configuration par défaut

Aucune

Mode de commande

Privileged Exec

Exemple

```
Console#show map ip dscp ethernet SNP1
DSCP mapping status: disabled

 Port        DSCP COS
 ----------- ---- ---
        SNP1    0   0
        SNP1    1   0
        SNP1    2   0
        SNP1    3   0
.
.
.
        SNP1    61   0
        SNP1    62   0
        SNP1    63   0
Console#
```

Commandes associées

map ip dscp (Global Configuration) (4-139)
map ip dscp (Interface Configuration) (4-140)

4.3.16 Commandes du port miroir

Cette section décrit la marche à suivre pour mettre le trafic d'un port source en miroir sur un port cible.

Commande	Fonction	Mode	Page
port monitor	Configure une session de mise en miroir	IC	4-143
show port monitor	Affiche la configuration d'un port de mise en miroir	PE	4-144

4.3.16.1 port monitor

Cette commande permet de configurer une session de mise en miroir. Utilisez la forme **no** pour supprimer une session de mise en miroir.

Remarque - Les commutateurs intégrés sur le châssis Sun Fire™ B1600 pour serveurs Blade sont chacun composés de deux puces de commutateurs reliées. Il n'est possible de mettre le trafic d'un port en miroir qu'en utilisant un autre port situé sur la même puce. Les ports NETP0 à NETP3 et SNP0 à SNP7 se trouvent sur l'une des puces. Les ports NETP4 à NETP7 et SNP8 à SNP15 se situent sur l'autre.

Syntaxe

port monitor *interface* [**rx** | **tx** | **both**]
no port monitor *interface*

- *interface* - **ethernet** *port-name*
  port-name : liaison descendante : SNP0-15 ; liaison ascendante : NETP0-7 ; gestion : NETMGT
  (Cette interface définit le port source.)
- **rx** : Mise en miroir des paquets reçus.
- **tx** : Mise en miroir des paquets transmis.
- **both** : Mise en miroir des paquets reçus comme des paquets transmis.

Configuration par défaut

Aucune session de mise en miroir n'est définie. Lorsque cette fonction est activée, la mise en miroir par défaut s'applique tant aux paquets reçus qu'aux paquets transmis.

Mode de commande

Interface Configuration (Ethernet, port de destination)

Utilisation de la commande

- Vous pouvez mettre le trafic provenant d'un port source en miroir sur un port cible pour une analyse en temps réel. Vous pouvez attacher un analyseur logique ou une sonde RMON au port de destination et étudier le trafic passant par le port source sans influer sur celui-ci.
- Pour définir le port de destination, spécifiez une interface Ethernet.

Exemple

L'exemple suivant met tous les paquets du port SNP6 en miroir sur le port NETP2 :

```
Console(config)#interface ethernet NETP2
Console(config-if)#port monitor ethernet SNP6 both
Console(config-if)#
```

Commandes associées

show port monitor (4-144)

4.3.16.2 show port monitor

Cette commande vous permet de consulter les informations de mise en miroir.

Syntaxe

show port monitor [*interface*]

interface - **ethernet** *port-name*
port-name : liaison descendante : SNP0-15 ; liaison ascendante : NETP0-7 ; gestion : NETMGT
(Cette interface définit le port source.)

Configuration par défaut

Affiche toutes les sessions

Mode de commande

Privileged Exec

Utilisation de la commande

Cette commande affiche le port source, le port cible ainsi que le mode de mise en miroir actuellement configurés (à savoir, RX, TX, RX/TX).

Exemple

L'exemple suivant affiche la mise en miroir configurée du port SNP6 sur le port NETP2 :

```
Console(config)#interface ethernet NETP2
Console(config-if)#port monitor ethernet SNP6
Console(config-if)#end
Console#show port monitor
Port Mirroring
-------------------------------------
 Destination port(listen port):NETP2
 Source port(monitored port)  :SNP6
 Mode                         :RX/TX
Console#
```

Commandes associées

port monitor (4-143)

4.3.17 Commandes de regroupement des ports

Il est possible de rassembler les ports de manière statique sous la forme d'une liaison groupée afin d'augmenter la bande passante d'une connexion réseau ou de garantir une reprise en cas de panne. Toutefois, vous pouvez également recourir au protocole LACP (Link Aggregation Control Protocol) afin de négocier automatiquement une liaison groupée entre le commutateur et un autre périphérique réseau. Pour les groupes statiques, les commutateurs doivent appartenir au même type. En revanche, pour les groupes dynamiques, il suffit que les commutateurs soient compatibles avec le protocole LACP. Ce commutateur peut accepter jusqu'à six groupes. Par exemple, un groupe composé de deux ports à 1000 Mbps peut prendre en charge une bande passante consolidée de 4 Gps lorsqu'il fonctionne en duplex.

Commande	Fonction	Mode	Page
Commandes de configuration manuelle			
interface port-channel	Configure un groupe et passe en mode de configuration d'interface pour celui-ci.	GC	4-74
channel-group	Ajoute un port à un groupe	IC	4-146
Commande de configuration dynamique			
Lacp	Configure le protocole LACP pour l'interface courante	IC	4-147
Commande d'affichage de l'état du groupe			
show interfaces status port-channel	Affiche des informations sur le groupe.	NE, PE	4-83

Directives régissant la création de groupes

- Terminez la configuration des groupes de ports avant de connecter les câbles réseau correspondants entre les commutateurs pour éviter de créer une boucle.
- Un groupe peut contenir jusqu'à quatre ports à liaisons ascendantes ou deux ports à liaison descendante.
- Les ports situés aux deux extrémités d'une connexion doivent être configurés comme ports du groupe.
- Tous les ports d'un groupe doivent être configurés d'une manière identique, en ce compris leur mode de communication (vitesse, mode duplex et contrôle de flux), leurs affectations au VLAN et leurs paramètres CdS.
- Tous les ports d'un groupe doivent être traités comme un ensemble lorsqu'ils sont déplacés depuis/vers un VLAN, lui sont ajoutés ou en sont supprimés par le biais du canal (port-channel) spécifié.
- Les paramètres STP, VLAN et IGMP ne peuvent être définis que pour l'ensemble du groupe par l'intermédiaire du canal (port-channel) spécifié.

4.3.17.1 channel-group

Cette commande permet d'ajouter un port à un groupe statique. Utilisez la forme **no** pour supprimer un port d'un groupe.

Syntaxe

channel-group *channel-id*
no channel-group

channel-id : Index du groupe (Plage : 1-6)

Configuration par défaut

Le port courant est ajouté à ce groupe.

Mode de commande

Interface Configuration (Ethernet)

Utilisation de la commande

- Lorsque vous configurez des groupes statiques, vous ne pouvez relier que des commutateurs du même type.
- La commande **no channel-group** permet de supprimer un groupe de ports d'un groupe.
- La commande **no interfaces port-channel** permet de supprimer un groupe du commutateur.

Exemple

L'exemple suivant crée un groupe 1, puis y ajoute le port NETP2 :

```
Console(config)#interface port-channel 1
Console(config-if)#exit
Console(config)#interface ethernet NETP2
Console(config-if)#channel-group 1
Console(config-if)#
```

4.3.17.2 lacp

Cette commande vous permet d'activer le protocole LACP (Link Aggregation Control Protocol) 802.3ad pour l'interface courante. Utilisez la forme **no** pour désactiver cette fonction.

Syntaxe

lacp
no lacp

Configuration par défaut

Activé

Mode de commande

Interface Configuration (Ethernet)

Utilisation de la commande

- Les ports situés aux deux extrémités d'un groupe LACP doivent être configurés en duplex, que ce soit en mode forcé ou en auto-négociation.
- Un groupe formé avec un autre commutateur à l'aide du protocole LACP reçoit automatiquement la première ID port-channel disponible.
- Si le commutateur cible a également activé le LACP sur les ports connectés, le groupe est activé automatiquement.
- Si plus de quatre ports attachés au même commutateur cible ont un LACP actif, les ports supplémentaires passent en mode veille et ne sont activés que si l'une des liaisons actives tombe en panne.

Exemple

L'exemple suivant affiche le protocole LACP activé sur les ports NETP0-2. Etant donné qu'il a également été activé sur les ports situés à l'autre extrémité des liaisons, la commande **show interfaces status port-channel 1** indique que le groupe Trunk1 a été établi.

```
Console(config)#interface ethernet NETP0
Console(config-if)#lacp
Console(config-if)#exit
Console(config)#interface ethernet NETP1
Console(config-if)#lacp
Console(config-if)#exit
Console(config)#interface ethernet NETP2
Console(config-if)#lacp
Console(config-if)#exit
Console(config)#exit
Console#show interfaces status port-channel 1
Information of Trunk 1
Basic information:
  Port type: 1 000t
  Mac address: 00-00-e8-00-00-0b
 Configuration:
  Name:
  Port admin status: Up
  Speed-duplex: Auto
  Capabilities: 10half, 10full, 100half, 100full, 1000full
  Flow control status: Disabled
 Current status:
  Created by: Lacp
  Link status: Up
  Operation speed-duplex: 1000full
  Flow control type: None
  Member Ports: NETP0, NETP1, NETP2,
Console#
```

PART III Annexes

Cette section propose des informations complémentaires sur les sujets suivants.

Base d'informations de gestion

Dépannage

Caractéristiques physiques

ANNEXE **A**

Base d'informations de gestion

Une station de gestion SNMP peut configurer et contrôler des périphériques réseau en définissant ou en lisant les variables relatives à ceux-ci dans la Base d'informations de gestion (MIB). Les principaux groupes de MIB pris en charge par ce commutateur sont répertoriés dans la présente annexe. De même, remarquez que les variables MIB spécifiques utilisées pour chaque tâche de configuration sont répertoriées dans chapitre 3, « Présentation des opérations de gestion ».

A.1 MIB prises en charge

Les MIB standard sont répertoriées dans la table suivante.

N° RFC	Titre	Groupes pris en charge
1213	MIB-II.	• system group • interfaces group • ip group • icmp group • system group • udp group • snmp group
1493	Bridge MIB	• dot1dBase group • dot1dStp group • dot1dTp group • dot1dStatic group
2863	Interfaces Evolution MIB	• ifXTable group • ifStackTable group

N° RFC	Titre	Groupes pris en charge
2819	RMON MIB	• statistics group • history group • alarm group • event group
2618	RADIUS MIB	• radiusAuthClientMIB
2665	Etherlike MIB	• dot3StatsTable group
2737	Entity MIB	• entityPhysical group
2674	P-bridge	• dot1dExtBase group • dot1dPriority group • dot1dGarp group
2674	Q-bridge	• dot1qBase group • dot1qTp group • dot1qStatic group • dot1qVlan

Les MIB Sun Private Enterprise sont répertoriées ci-dessous.

Titre	Version
CSSP.MIB	01.00.00

A.2 Interruptions prises en charge

Les interruptions SNMP prises en charge sont les suivantes :

N° RFC	Titre
RFC 1215 (SNMPv1), RFC 1907 (SNMPv2c)	• coldStart • linkDown • linkUp • authenticationFailure
RFC 1493	• newRoot • topologyChange
RFC 2819	• risingAlarm • fallingAlarm

L'interruption Sun Private Enterprise prise en charge est la suivante :

N° RFC	Titre
CSSP.MIB	• swPowerStatusChangeTrap

ANNEXE **B**

Dépannage

Si vous éprouvez des difficultés à vous connecter au réseau, vérifiez le câblage afin de vous assurer que le périphérique concerné est correctement raccordé au réseau. Ensuite, reportez-vous à « Diagnostic des voyants du commutateur », à la page B-1 pour vérifier que le port correspondant du commutateur fonctionne normalement.

Si vous éprouvez des difficultés à vous connecter à l'interface de gestion, reportez-vous au tableau de dépannage présenté sous « Accès à l'interface de gestion », à la page B-2.

B.1 Diagnostic des voyants du commutateur

Si vous avez connecté un périphérique à un port du commutateur, mais que le voyant de la liaison est éteint, vérifiez les points suivants :

- Le câble doit être raccordé au commutateur et au périphérique correspondant.
- Le type de câble utilisé doit être adéquat et sa longueur ne peut pas dépasser les limites spécifiées.
- L'adaptateur du périphérique raccordé et les câbles doivent être exempts de défauts. Si nécessaire, remplacez l'adaptateur ou le câble défectueux.

Tous les composants système doivent avoir été correctement installés. Si un câblage réseau semble mal fonctionner, testez-le dans un autre environnement, où vous êtes sûr que tous les autres composants fonctionnent correctement.

B.2 Diagnostic des connexions aux ports

Si un port ne fonctionne pas, vérifiez les points suivants :

- Les câbles sont bien fixés et connectés aux bons ports aux deux extrémités de la liaison.
- L'état du port (Admin) est activé, et la fonction d'auto-négociation est activée, ou les ports aux deux extrémités de la liaison sont configurés à la même vitesse et au même mode duplex. Reportez-vous à la rubrique « Configuration du port », à la page 3-80 pour plus d'informations.

B.3 Accès à l'interface de gestion

Vous pouvez accéder à l'interface de gestion du commutateur depuis n'importe quel endroit du réseau connecté à l'aide de Telnet, d'un navigateur Web ou de tout logiciel de gestion réseau basé sur le SNMP. Si vous éprouvez des difficultés à accéder à l'interface de gestion, reportez-vous aux informations de dépannage présentées ci-dessous.

Si vous ne pouvez pas vous connecter par le biais de Telnet, d'un navigateur Web ou d'un logiciel SNMP, vérifiez les points suivants :

- Le châssis du serveur est mis sous tension.
- Le câblage réseau entre la station de gestion et le commutateur est correct.
- Vous disposez d'une connexion réseau valable au commutateur et le port utilisé n'a pas été déconnecté. Voir « Configuration du port », à la page 3-80.
- S'il n'existe que des commutateurs de Couche 2 entre la station de gestion et le châssis du serveur, vérifiez les points suivants :
  - Le VLAN de gestion du commutateur est configuré avec une adresse IP et un masque de sous-réseau valables ;
  - La station de gestion possède une adresse IP dans le même sous-réseau que le réseau local virtuel de gestion ;
  - La station de gestion est connectée à un port du commutateur membre du VLAN de gestion ;
  - Les ports raccordant les commutateurs intermédiaires du réseau sont marqués et appartiennent au VLAN de gestion.

- S'il existe un ou plusieurs communicateurs de Couche 3 entre la station de gestion et le châssis du serveur, vérifiez les points suivants :
  - le VLAN de gestion du commutateur est configuré avec une adresse IP, un masque de sous-réseau et une passerelle par défaut valables ;
  - La station de gestion possède une adresse IP, un masque de sous-réseau et une passerelle par défaut valables ;
  - La station de gestion est connectée à un port du commutateur membre du VLAN de gestion ;
  - les ports raccordant les commutateurs intermédiaires et le(s) commutateur(s) de couche 3 dans le réseau sont marqués et appartiennent au VLAN de gestion.
- Si vous n'arrivez pas vous connecter à l'aide de Telnet, il est possible que vous ayez dépassé le nombre maximal de sessions Telnet simultanées autorisées. Essayez de vous reconnecter ultérieurement.

Si vous ne pouvez pas accéder au programme de configuration intégré par le biais d'une connexion à un port série, vérifiez les points suivants :

- Utilisez le câble DB-9-à-RJ-45 fourni avec le Châssis Sun Fire™ B1600 pour serveurs Blade pour raccorder votre terminal ou ordinateur au port série du module SSC.
- Assurez-vous d'avoir définir le programme émulateur de terminal à VT100 compatible, 8 bits de données, 1 bit d'arrêt, aucune parité et 9600 bps.
- Vérifiez que le câble série faux modem est conforme aux brochages présentés à l'annexe B.

B.4 Utilisation des journaux système

Si une panne survient, reportez-vous aux autres manuels du châssis du serveur afin de vous assurer que le problème rencontré est bien causé par le commutateur. Si tel semble être le cas, procédez comme suit.

1. Activez la journalisation.
2. Définissez l'émission de messages d'erreurs afin qu'elle inclue toutes les catégories.
3. Désignez l'hôte SNMP qui doit recevoir les messages d'erreur.
4. Répétez la séquence des commandes ou actions qui ont conduit à l'erreur.
5. Dressez une liste des commandes ou des circonstances qui ont entraîné la panne. Répertoriez également les messages d'erreurs affichés.
6. Contactez le service client.

Exemple

```
Console(config)#logging on
Console(config)#logging history flash 7
Console(config)#snmp-server host 10.1.0.23
.
.
.
```

B.4.1 Journaux

Les messages générés par ce commutateur sont répertoriés dans le tableau suivant :

TABLEAU B-1 Journaux

Message	Description	Niveau*
Notification System coldStart	Amorçage à froid du commutateur	5
Notification System warmStart	Amorçage à chaud du commutateur	5
Notification Unit 1 Port YY link-up	Liaison ascendante du port	6
Notification Unit 1 Port YY link-down	Liaison descendante du port	6
Notification Trunk 1 link-up	Liaison ascendante du groupe	6
Notification Trunk 1 link-down	Liaison descendante du groupe	6
Notification VLAN XX link-up	Liaison ascendante du VLAN	6
Notification VLAN XX link-down	Liaison descendante du VLAN	6
Notification Authentication failure	Echec de l'authentification de l'accès SNMP	6
Notification STA root change	Modification de la racine STA	6
Notification STA topology change	Modification de la topologie STA	6
Notification RMON rising alarm	Alerte d'augmentation RMON	6
Notification RMON falling alarm	Alerte de chute RMON	6

Unit 1 Port YY signifie unité 1, port YY (YY : 1 à 25).
VLAN XX signifie un identificateur de VLAN quelconque (XX : 1 à 4094).

* Niveau du message syslog (Voir « logging history », à la page 4-31.)

B.5 Messages d'erreur

B.5.1 Détection des erreurs de ligne de commande

Si le commutateur décèle une saisie incorrecte dans la ligne de commande, il affiche un « ^ » en regard de l'erreur détectée. Par exemple,

```
Console#show interfaces statuss e 1/1
                                 ^
% Invalid input detected at '^' marker.
```

B.5.2 Erreurs système

Les principaux messages d'erreur générés par ce commutateur sont répertoriés dans le tableau suivant. Pour déterminer le niveau des messages émis par le commutateur, consultez « logging history », à la page 4-31.

TABLEAU B-2 Messages d'erreur système

Message	Description	Niveau*
<module> create task fail.	Le module logiciel spécifié ne peut pas créer la tâche.	2
<module> task idle too long.	Le module logiciel spécifié est resté inactif trop longtemps.	2
Allocate <string> memory fail.	L'allocation de mémoire a échoué pour la <chaîne> spécifiée.	2
Free <string> memory fail.	La mémoire libre a échoué pour la <chaîne> spécifiée.	2
<string> switch to default.	La valeur spécifiée n'est pas valable ou pas prise en charge ; la valeur par défaut est utilisée. (Veuillez vous reporter à l'aide en ligne ou au manuel pour obtenir de plus amples informations sur les valeurs autorisées).	3

module signifie le module logiciel du commutateur (par exemple, STA, VLAN, XFER, TRAP ou RMON).
string indique la valeur spécifiée pour un paramètre de configuration.

* Niveau du message syslog (Voir « logging history », à la page 4-31.)

B.5.3 Erreurs de ligne de commande

Les messages d'erreur générés par ce commutateur pour l'interface de ligne de commande sont répertoriés dans le tableau suivant. Remarquez que ces messages ne sont pas consignés dans le fichier journal.

TABLEAU B-3 Messages d'erreur de ligne de commande

Message	Description
Ambiguous command: <chaîne>	Cette commande est ambiguë.
Clear dynamic address error.	L'adresse dynamique n'a pas pu être supprimée.
CLI internal error - contact your local service provider.	Une erreur interne à l'ILC est survenue.
Copy error.	La copie a échoué.
Exec-timeout could not be disabled for vty session.	La session Telnet ne peut pas désactiver exec-timeout.
Factory default configuration file cannot be deleted.	Le fichier par défaut ne peut pas être supprimé.
Factory default configuration file cannot be replaced.	Le fichier par défaut ne peut pas être remplacé.
Failed to allocate resource.	Les ressources sont insuffisantes.
Failed to get <chaîne>	La commande d'affichage a échoué.
Failed to set <chaîne>	La commande de configuration a échoué.
Failed to write certificate file to flash.	Le fichier du certificat comporte une erreur, une erreur relative au fichier de clé privée (par exemple, un mot de passe incorrect) ou la clé privée ne correspond pas à la clé publique du certificat.
Incomplete command.	La commande est incomplète.
Insufficient memory.	La mémoire est insuffisante.
Insufficient memory to display or save running config.	L'espace disque est insuffisant pour collecter toutes les informations.
Invalid file name.	Le nom de fichier entré n'est pas valable.
Invalid input.	La saisie clavier est erronée.
Invalid input detected at '^' marker.	Cette commande n'est pas valable.
Invalid parameter.	Le paramètre Ping est erroné.
Invalid parameter value/range. Type "?" to get more detail information.	La valeur ou la longueur de la chaîne de caractères n'est pas autorisée.
Invalid TFTP server IP address.	L'adresse IP TFTP est erronée.

TABLEAU B-3 Messages d'erreur de ligne de commande

Message	Description
Not enough resources; please try later.	La fonction Ping ne dispose d'aucune ressource.
No such file.	Le système ne trouve pas le fichier.
No such VLAN.	Ce réseau local virtuel n'existe pas.
Port <nom du port> does not exist.	Ce nom de port n'existe pas.
Port <nom du port> is an ethernet port.	Ce port est un port Ethernet.
Port <nom du port> is not present.	Ce port n'est pas présent lorsque vous passez en mode interface.
Port <nom du port> unknown.	Ce port est inconnu.
Session terminated.	L'ILC a quitté la session courante.
Session timed out.	La session a expiré.
Startup file cannot be deleted.	Le fichier de démarrage ne peut pas être effacé.
This command for console only.	Le mode Ligne (vty) ne peut pas utiliser les commandes de configuration de la console.
This command is only valid for adding a single port to a trunk.	Cette commande ne permet d'ajouter qu'un seul port à un groupe.
This command is only valid for the name of a single port.	Lorsque vous définissez la description des ports, il n'est pas possible d'en sélectionner plusieurs.
This command is not supported for management port in current release.	La commande « no switchport allow vlan » ne peut pas être utilisée pour le port de gestion.
ID du groupe : <groupe> is out of range.	L'identificateur de ce groupe n'est pas autorisé.
Trunk <groupe> does not exist.	Ce groupe n'existe pas.
Trunk <groupe> is a normal trunk.	Ce groupe est un groupe normal.
Trunk with no members cannot be displayed.	Il est impossible de configurer ou d'afficher les membres de ce groupe.
Type "show ?" for a list of subcommands.	Il vous suffit d'entrer la commande « show ».
Unknown error.	Erreur inconnue.
Unrecognized command.	Cette commande n'a pas pu être reconnue.

<chaîne> indique la valeur spécifiée pour une commande.

B.5.4 Erreurs de l'interface Web

Les messages d'erreur générés par ce commutateur pour l'interface Web sont répertoriés dans le tableau suivant. Remarquez que ces messages ne sont pas consignés dans le fichier journal.

TABLEAU B-4 Messages d'erreur afférents à l'interface Web

Menu	Message	Description
Switch Setup (Configuration du commutateur)		
System Identity (Identité système)	User privileges are not enough to perform this operation.	Vous ne disposez pas des droits requis pour exécuter cette opération.
Network Identity (Identité du réseau)	Current IP Address Mode is not DHCP or BOOTP.	Lorsque vous redémarrez le DHCP, le commutateur doit se trouver en mode DHCP ou BOOTP.
	Data is invalid.	Données non valables. Erreur générale.
	Set DHCP Client-ID error.	La définition de l'identificateur du client DHCP a échoué.
	User privileges are not enough to perform this operation.	Vous ne disposez pas des droits requis pour exécuter cette opération.
Software (Logiciel)	Data is invalid.	Données non valables. Erreur générale.
	Please input a destination file.	Saisissez le nom du fichier de destination à télécharger.
	Please input a source file.	Saisissez le nom du fichier source à télécharger.
	Please input or select a destination file.	Saisissez ou sélectionnez le nom d'un fichier à télécharger ou à charger.
	Please select a file.	Sélectionnez un fichier à télécharger ou à charger.
	System will be restarted...	Le système va être redémarré.
	User privileges are not enough to perform this operation.	Vous ne disposez pas des droits requis pour exécuter cette opération.
Switch Config (Configuration du commutateur)		
Security (Sécurité)	Cannot add user.	Le système n'a pas pu ajouter l'utilisateur. Le nom de l'utilisateur n'est pas valable ou le nombre maximum d'utilisateurs a été dépassé.

TABLEAU B-4 Messages d'erreur afférents à l'interface Web

Menu	Message	Description
	Cannot set password for user.	Le système n'a pas pu définir le mot de passe de l'utilisateur. Le mot de passe n'est pas valable.
	Cannot set user privilege.	Le système n'a pas pu définir les droits utilisateur en raison d'un problème dans la table des utilisateurs.
	Cannot set user status.	Le système n'a pas pu définir l'état de l'utilisateur en raison d'un problème dans la table des utilisateurs.
	User does not exist.	L'utilisateur n'existe pas. La table des utilisateurs présente un problème.
Communication	Community String cannot contain spaces.	La chaîne communautaire ne peut pas contenir d'espaces.
	Community table is full or data is invalid.	La table communautaire est remplie ou les données ne sont pas valables.
	Data is invalid.	Données non valables. Erreur générale.
	Illegal SNMP trap IP address.	Ce format de l'adresse IP n'est pas autorisé.
	Please select a Community String.	Sélectionnez une chaîne communautaire à supprimer.
	Please type a Community String.	Saisissez une chaîne communautaire à ajouter.
	Trap Manager table is full or data is invalid.	La table des gestionnaires d'interruptions est remplie ou les données ne sont pas valables.
	User privileges are not enough to perform this operation.	Vous ne disposez pas des droits requis pour exécuter cette opération.
	You must specify an IP trap community string.	Saisissez une chaîne communautaire d'interruptions IP à ajouter.
Security (Sécurité)	Authentication type doesn't exist.	L'un des types d'authentification local, TACACS ou RADIUS n'est pas pris en charge.
	Data is invalid	Données non valables. Erreur générale.
	Illegal IP address.	Le format de l'adresse IP n'est pas autorisé.
	Number of Server Transmits is out of range.	Le nombre de répétitions RADIUS ne se situe pas dans la plage des valeurs autorisées.
	Password too long.	La longueur maximale du mot de passe a été dépassée.
	Please input username.	Saisissez un nom d'utilisateur pour ajouter un utilisateur.
	Please select an user	Sélectionnez un utilisateur à supprimer ou dont vous souhaitez modifier le mot de passe.
	RADIUS KEY is invalid	La clé de chiffrement RADIUS n'est pas valable.

TABLEAU B-4 Messages d'erreur afférents à l'interface Web

Menu	Message	Description
	Server Port Number is out of range.	Le numéro du port RADIUS ne se situe pas dans la plage des valeurs autorisées.
	Select a privilege level.	Sélectionnez un niveau d'accès pour ajouter un utilisateur.
	TACACS PORT is invalid	Le port TACACS n'est pas valable.
	TACACS KEY is invalid	La clé TACACS n'est pas valable.
	Timeout is out of range.	Le dépassement du délai imparti RADIUS ne se situe pas dans la plage des valeurs autorisées.
	User privileges are not enough to perform this operation.	Vous ne disposez pas des droits requis pour exécuter cette opération.
VLAN	Cannot create VLAN.	Le système n'a pas pu créer le VLAN. L'identificateur du VLAN n'est pas valable, ou le nombre maximal de VLAN pris en charge a été dépassé.
	Cannot set VLAN name.	Ce nom de VLAN n'est pas valable.
	Cannot set VLAN status.	Il est impossible de désactiver le VLAN 1 ou le VLAN défini comme VLAN naturel (PVID) du port de gestion.
	Cannot delete VLAN.	Il est impossible de supprimer des VLAN comportant des membres ou un VLAN défini en tant que VLAN naturel (PVID) d'une interface.
	Data is invalid	Données non valables. Erreur générale.
	User privileges are not enough to perform this operation.	Vous ne disposez pas des droits requis pour exécuter cette opération.
Membership (Appartenance)	Data is invalid.	Données non valables. Erreur générale.
	User privileges are not enough to perform this operation.	Vous ne disposez pas des droits requis pour exécuter cette opération.
Broadcast & Multicast (Diffusion et Multidiffusion)		
Broadcast Parameters (Paramètres de diffusion)	Threshold is out of range.	La limite maximale du seuil des orages de diffusion a été dépassée.
	User privileges are not enough to perform this operation.	Vous ne disposez pas des droits requis pour exécuter cette opération.
IGMP Parameters (Paramètres IGMP)	Please enter a valid version.	Entrez une version valable.
	Query count is out of range.	Le nombre de requêtes ne se situe pas dans la plage des valeurs autorisées.

TABLEAU B-4 Messages d'erreur afférents à l'interface Web

Menu	Message	Description
	Query interval is out of range.	L'intervalle des requêtes ne se situe pas dans la plage des valeurs autorisées.
	Query timeout is out of range.	L'expiration des requêtes ne se situe pas dans la plage des valeurs autorisées.
	Report delay is out of range.	Le retard de notification ne se situe pas dans la plage de valeurs autorisées.
	User privileges are not enough to perform this operation.	Vous ne disposez pas des droits requis pour exécuter cette opération.
Multicast Router Ports (Ports des routeurs multidestinataires)	Data is invalid.	Données non valables. Erreur générale.
	Please select a port	Sélectionnez des ports à ajouter (supprimer) au (du) routeur multidestinataire.
	User privileges are not enough to perform this operation.	Vous ne disposez pas des droits requis pour exécuter cette opération.
Services multidestinataires	Data is invalid.	Données non valables. Erreur générale.
	Igmp group member is null.	Sélectionnez un membre du groupe IGMP dans la liste.
	Illegal IP address.	Le format de l'adresse IP n'est pas autorisé.
	Select a port or trunk	Sélectionnez des ports à ajouter (supprimer) aux (des) ports statiques du VLAN.
	User privileges are not enough to perform this operation.	Vous ne disposez pas des droits requis pour exécuter cette opération.
Spanning Tree		
Basic Configuration (Configuration de base)	Data is invalid.	Données non valables. Erreur générale.
	Priority is out of range.	La priorité ne se situe pas dans la plage des valeurs autorisées.
	User privileges are not enough to perform this operation.	Vous ne disposez pas des droits requis pour exécuter cette opération.
Configuration avancée	Data is invalid.	Données non valables. Erreur générale.
	User privileges are not enough to perform this operation.	Vous ne disposez pas des droits requis pour exécuter cette opération.

TABLEAU B-4 Messages d'erreur afférents à l'interface Web

Menu	Message	Description
Class of Service (Classe de service)		
Basic Traffic Priorisation (Priorisation de base du trafic)	Cos Value is out of range.	La valeur CdS ne se situe pas dans la plage des valeurs autorisées.
	Data is invalid.	Données non valables. Erreur générale.
	Priority is out of range.	La priorité ne se situe pas dans la plage des valeurs autorisées.
	Queue weight must be in a order of Q0<=Q1<=Q2<=Q3	Le poids de la file d'attente n'est pas valable.
	Traffic Class is out of range.	La classe de trafic ne se situe pas dans la plage des valeurs autorisées.
	User privileges are not enough to perform this operation.	Vous ne disposez pas des droits requis pour exécuter cette opération.
Layer 3/4 Traffic Prioritisation (Priorisation du trafic de la couche 3/4)	Cos Value is out of range.	La valeur CdS ne se situe pas dans la plage des valeurs autorisées.
	Please select IP Precedence or DSCP mode	Sélectionnez l'une de ces options lorsque le service de priorité est activé.
	Traffic Class is out of range.	La classe de trafic ne se situe pas dans la plage des valeurs autorisées.
	User privileges are not enough to perform this operation.	Vous ne disposez pas des droits requis pour exécuter cette opération.
Address Tables (Tables d'adressage)	Aging time is out of range.	Le délai maximal d'obsolescence des adresses est dépassé.
	User privileges are not enough to perform this operation.	Vous ne disposez pas des droits requis pour exécuter cette opération.
Up Links, Down Links (Liaisons ascendantes/descendantes)		
Status (Etat)	Cannot set port capabilities.	Le système n'a pas pu définir les capacités du port. La vitesse et le mode duplex sont incorrects pour le port spécifié.
	Data is invalid.	Données non valables. Erreur générale.
	User privileges are not enough to perform this operation.	Vous ne disposez pas des droits requis pour exécuter cette opération.

TABLEAU B-4 Messages d'erreur afférents à l'interface Web

Menu	Message	Description
Link Aggregation (Regroupement des liaisons)	Cannot add trunk. The specified trunk is full or data is invalid.	Le groupe spécifié est rempli, ou les données ne sont pas valables.
	Cannot create trunk.	Le nombre maximal de groupes a été dépassé.
	Cannot remove trunk.	Le système n'a pas pu supprimer le groupe en raison d'un problème dans la table des groupes.
	Cannot remove trunk member. Data is invalid.	Le système n'a pas pu supprimer le membre du groupe en raison d'un problème dans la table des groupes.
	Cannot set trunk status.	L'activation du protocole LACP pour un membre statique du groupe est impossible.
	Data is invalid.	Données non valables. Erreur générale.
	User privileges are not enough to perform this operation.	Vous ne disposez pas des droits requis pour exécuter cette opération.
VLAN	Data is invalid.	Données non valables. Erreur générale.
	Please enter a valid PVID.	Le PVID n'est pas valable. Sélectionnez-en un autre.
	Please enter a valid timer.	L'horloge n'est pas valable. Sélectionnez-en une autre.
	Table is full or data is invalid.	La table est remplie, ou les données ne sont pas valables.
	User privileges are not enough to perform this operation.	Vous ne disposez pas des droits requis pour exécuter cette opération.
Address Filtering (Filtrage des adresses)	Data is invalid.	Données non valables. Erreur générale.
	Please enter a valid MAC address.	L'adresse MAC n'est pas valable.
	Please enter a valid VLAN ID.	L'ID du VLAN n'est pas valable.
	Table is full or data is invalid.	La table est remplie, ou les données ne sont pas valables.
	User privileges are not enough to perform this operation.	Vous ne disposez pas des droits requis pour exécuter cette opération.
Spanning Tree	Data is invalid.	Données non valables. Erreur générale.
	User privileges are not enough to perform this operation.	Vous ne disposez pas des droits requis pour exécuter cette opération.
Config	Path cost is out of range.	Le coût de résolution ne se situe pas dans la plage des valeurs autorisées.

TABLEAU B-4 Messages d'erreur afférents à l'interface Web

Menu	Message	Description
	Priority is out of range.	La priorité ne se situe pas dans la plage des valeurs autorisées.
Port	Path cost is out of range.	Le coût de résolution ne se situe pas dans la plage des valeurs autorisées.
	Priority is out of range.	La priorité ne se situe pas dans la plage des valeurs autorisées.
	User privileges are not enough to perform this operation.	Vous ne disposez pas des droits requis pour exécuter cette opération.
Management Ports (Ports de gestion)		
VLAN	Data is invalid.	Données non valables. Erreur générale.
	Please enter a valid PVID.	Le PVID n'est pas valable. Sélectionnez-en une autre.
	Please enter a valid timer.	L'horloge n'est pas valable. Sélectionnez-en une autre.
	Table is full or data is invalid.	La table est remplie, ou les données ne sont pas valables.
	User privileges are not enough to perform this operation.	Vous ne disposez pas des droits requis pour exécuter cette opération.
Packet Filtering (Filtrage des paquets)	User privileges are not enough to perform this operation.	Vous ne disposez pas des droits requis pour exécuter cette opération.
Monitoring (Surveillance)		
Port Mirroring (Mise en miroir des ports)	Data is invalid.	Données non valables. Erreur générale.
	User privileges are not enough to perform this operation.	Vous ne disposez pas des droits requis pour exécuter cette opération.
Logs (Journaux)	Data is invalid.	Données non valables. Erreur générale.
	User privileges are not enough to perform this operation.	Vous ne disposez pas des droits requis pour exécuter cette opération.

ANNEXE **C**

Caractéristiques physiques

C.1 Architecture du commutateur

Ports

Liaisons réseau ascendantes : 8 1000BASE-T
Panneau central : Liaisons série descendantes 16 Gigabit (pour les serveurs Blade)
Canal de gestion : 1 10/100BASE-TX, 1 port console (RJ-45 série)

Interface réseau

Ports 10/100/1000Base-T NETP0-7 :
Connecteur RJ-45, auto-négociation, auto MDI/MDI-X
Câblage : Câble UTP 10BASE-T: 100-ohm ; Catégories 3, 4, 5
Câble UTP 100BASE-TX : 100-ohm ; Catégorie 5
Câble UTP 1000BASE-TX : 100-ohm ; Catégorie 5 ou 5e

Architecture du tampon

Ports à liaison ascendante/descendante : 1 Mo partagé

Bande passante agrégée

48 Gbps

Base de données de commutation

32 000 Entrées d'adressage MAC

Voyants

SSC : Actif, Intervention requise, Prêt au retrait
Ports Ethernet : Liaison/Actif, Vitesse

C.2 Fonctions de gestion

Gestion intrabande

Telnet, HTTP basé sur le Web ou SNMP

Gestion hors-bande

Signalisation RS-232 sur un port de console RJ-45

Chargement du logiciel

TFTP intrabande ou XModem hors-bande

Prise en charge de la MIB

SNMP v1/v2 (RFC 1215, 1907), MIB II (RFC 2863), Bridge MIB (RFC 1493), Etherlike MIB (RFC 1643/2665), RMON (RFC 2819 groups 1,2,3,9), IEEE 802.1Q VLAN (RFC 2674), IEEE 802.3ad LACP, private MIB

Prise en charge RMON

Groupes 1, 2, 3, 9 (Statistiques, Historique, Alerte, Événement)

Autres fonctions

Groupes de ports (Statique et LACP)
Mise en miroir des ports
Sécurité des ports
Client d'authentification RADIUS

C.3 Caractéristiques physiques

Poids

2,08 Kg

Dimensions

27,5 x 20,3 x 4,3 cm

C.4 Alimentation

Tension de fonctionnement

+12 V CC

Tension maximale

5,2 A

Consommation électrique

62 Watts maximum

Dissipation de chaleur

211 BTU/h maximum

C.5 Caractéristiques liées à l'environnement

Température

Fonctionnement : 5° C à 45° C
Stockage : -40 °C à 70 °C

Humidité

Fonctionnement : 10 % à 90 % (sans condensation)

C.6 Normes

IEEE 802.3 Ethernet, IEEE 802.3u Fast Ethernet, IEEE 802.3ab Gigabit Ethernet
Priorités du trafic et Protocole Spanning Tree IEEE 802.1D
Reconfiguration rapide (STP) IEEE 802.1w
Marques de priorité IEEE 802.1p, VLAN IEEE 802.1Q, marquage VLAN IEEE 802.3ac,
Contrôle de flux en mode full duplex IEEE 802.3x (ISO/IEC 8802-3)
Protocole LACP (Link Aggregation Control Protocol) IEEE 802.3ad,
SNMP (RFC 1215, 1907), RMON (RFC 2819 groupes 1,2,3,9), MIB II (RFC 2863),
Bridge MIB (RFC 1493), Etherlike MIB (RFC 1643/2665),
ARP (RFC 826), IGMP (RFC 1112), ICMP (RFC 792)

Glossaire

10BASE-T	Spécification IEEE 802.3 pour Ethernet 10 Mbps via deux paires de câbles UTP de catégorie 3, 4, ou 5.
100BASE-TX	Spécification IEEE 802.3u pour Fast Ethernet 100 Mbps via deux paires de câbles UTP de catégorie 5.
1000BASE-T	Spécification IEEE 802.3ab pour Gigabit Ethernet via deux paires de câbles UTP de catégorie 5, 5e 100-ohm.
1000BASE-X	Abréviation IEEE 802.3 désignant tout Gigabit Ethernet 1000 Mbps basé sur une signalisation 8B/10B.
Auto-négociation	Méthode de signalisation permettant à chaque noeud de sélectionner son mode opérationnel optimal (par exemple, 10 Mbps ou 100 Mbps ; semi duplex ou full duplex) sur la base des capacités du noeud auquel il est connecté.
Bande passante	Ecart entre les fréquences les plus élevées et les plus faibles disponibles pour les signaux réseaux. Egalement synonyme de vitesse réseau, vitesse réelle de transmission des données le long du câble.
Base d'informations de gestion (MIB)	Acronyme de Management Information Base (Base d'informations de gestion). Ensemble d'objets de base de données contenant des informations sur un périphérique spécifique.
BOOTP	Protocole d'amorçage utilisé pour charger le système d'exploitation sur les périphériques connectés au réseau.
Câble (STP) **à paire torsadée et blindée**	Câble à paire torsadée recouvert d'un feuillet d'aluminium externe ou d'un blindage en cuivre tressé conçus pour réduire l'absorption ou l'émission excessives de bruits.
Câble (UTP) **à paire torsadée non blindée.**	Câble composé de deux fils isolés, torsadés pour réduire les interférences électriques ; utilisé dans les câbles téléphoniques standard.

Collision Situation dans laquelle des paquets transmis par le biais du câble interfèrent les uns avec les autres. Leur interférence rend les deux signaux inintelligibles. Ceci ne s'applique qu'aux connexions en semi duplex.

Commutation multidestinataire Processus au cours duquel le commutateur filtre les trames multidestinataires entrantes pour les services auxquels aucun hôte connecté ne s'est enregistré, ou les transfère à tous les ports contenus dans le groupe de VLAN multidestinataires désigné.

Connecteur RJ-45 Connecteur pour paire de câbles torsadés.

Couche 2 Couche de liaison de données au protocole ISO 7-LDCP (Layer Data Communications Protocol). Celle-ci est reliée directement à l'interface matérielle des périphériques réseau et transfère le trafic sur la base des adresses MAC.

Couche 3 Couche réseau au protocole ISO 7-LDCP (Layer Data Communications Protocol). Cette couche traite les fonctions de routage relatives aux transferts de données d'un système ouvert à un autre.

CSMA/CD (Carrier Sense Multiple Access/Collision Detect) Méthode de communication employée par Ethernet et Fast Ethernet.

Domaine de collision Segment LAN CSMA/CD LAN unique.

Duplex Méthode de transmission permettant au commutateur et à la carte réseau de transmettre et de recevoir simultanément, en doublant efficacement la bande passante de la liaison.

Ethernet Système de communication réseau développé et normalisé par DEC, Intel et Xerox, utilisant la transmission de la bande de base, l'accès CSMA/CD, la topologie du bus logique ainsi qu'un câble coaxial. La nouvelle norme IEEE 802.3 propose une intégration au modèle OSI et étend la couche et le support physiques à l'aide de répétiteurs et de mises en oeuvre fonctionnant sur des câbles en fibre optique, coaxiaux fins et à paire torsadée.

Exploitation de la bande passante Pourcentage historique des paquets reçus comparé à la bande passante totale.

Fast Ethernet Système de communication réseau à 100 Mbps basé sur les méthodes d'accès Ethernet et CSMA/CD.

Filtrage multidestinataire IP Processus au cours duquel le commutateur peut transférer le trafic multidestinataire aux hôtes participants.

Generic Attribute Registration Protocol (GARP) Protocole utilisable par les stations terminales et les commutateurs pour enregistrer et propager des informations relatives à l'appartenance aux groupes multidestinataires dans un environnement commuté, de sorte que les trames de données multidestinataires ne soient propagées qu'aux segments d'un réseau local commuté contenant les stations terminales enregistrées. Auparavant, GARP signifiait « Group Address Registration Protocol ».

Gestion hors-bande Gestion du réseau depuis une station non raccordée au réseau.

Gestion intrabande Gestion du réseau depuis une station raccordée directement au réseau.

Gigabit Ethernet Système de communication réseau à 1000 Mbps basé sur les méthodes d'accès Ethernet et CSMA/CD.

Group Attribute Registration Protocol *Voir Generic Attribute Registration Protocol.*

Groupe de ports Méthode de regroupement de liaisons réseau permettant de générer une seule liaison logique à haute vitesse rassemblant plusieurs liaisons physiques plus lentes.

IEEE 802.1D Norme spécifiant une méthode générale pour l'utilisation des ponts MAC, y compris le protocole Spanning Tree.

IEEE 802.1Q Marquage VLAN : Définit les marques des trames Ethernet porteuses d'informations sur le réseau local virtuel. Il permet aux commutateurs d'affecter des stations terminales à différents LAN virtuels et définit une méthode standard permettant aux VLAN de communiquer sur des réseaux commutés.

IEEE 802.1p Norme IEEE garantissant la qualité des services (QdS) dans les réseaux Ethernet. Elle utilise des marques de paquets définissant jusqu'à huit classes de trafic et permettant aux commutateurs de transmettre les paquets sur la base de la priorité spécifiée par les marques.

IEEE 802.1w Norme IEEE pour le protocole Spanning Tree rapide (RSTP), destinée à remplacer IEEE 802.1D. RSTP fournit une convergence considérablement plus rapide pour les modifications de topologie.

IEEE 802.3 Définit l'accès multiple à l'analyse du signal porteur grâce à la méthode d'accès de détection de collisions (CSMA/CD) et aux spécifications de la couche physique.

IEEE 802.3ab Norme définissant la méthode d'accès CSMA/CD et les spécifications de la couche physique pour 1000BASE-T Fast Ethernet.

IEEE 802.3ac Norme définissant les extensions des trames pour le marquage VLAN.

IEEE 802.3u Norme définissant la méthode d'accès CSMA/CD et les spécifications de la couche physique pour 100BASE-TX Fast Ethernet.

IEEE 802.3x Norme définissant les requêtes d'arrêt/de démarrage des trames Ethernet ainsi que les horloges utilisées pour le contrôle de flux sur les liens en mode full duplex.

IEEE 802.3z Norme définissant la méthode d'accès CSMA/CD et les spécifications de la couche physique pour 1000BASE Gigabit Ethernet.

IGMP Snooping — Surveillance des paquets IGMP Query et IGMPE Report transférés entre les routeurs IP multidestinataires et les groupes d'hôtes IP multidestinataires afin d'identifier les membres des groupes IP multidestinataires.

Internet Control Message Protocol (ICMP) — Protocole généralement utilisé pour envoyer des messages d'échos (par exemple, pour vérifier l'état de la connexion) à des fins de contrôle.

Internet Group Management Protocol (IGMP) — Protocole à l'aide duquel les hôtes peuvent s'enregistrer auprès de leur routeur local pour les services multidestinataires. S'il existe plus d'un routeur multidestinataire sur un sous-réseau donné, l'un des routeurs devient le « requêteur » et se charge de conserver trace de l'appartenance aux groupes.

Link Aggregation Control Protocol (LACP) — Protocole permettant aux ports de négocier automatiquement une liaison groupée avec les ports configurés en LACP d'un autre périphérique.

Media Access Control (MAC) — Portion du protocole réseau régissant l'accès au support de transmission, facilitant l'échange de données entre des noeuds du réseau.

Mise en miroir des ports — Méthode par le biais de laquelle les données d'un port cible sont mises en miroir sur un port de contrôle pour être soumises à un analyseur logique ou à une sonde RMON à des fins de dépannage. Cette opération permet d'étudier les données du port cible sans interrompre leur flux.

Ports commutés — Ports se trouvant sur des domaines de collision ou des segments LAN distincts.

Protocole DHCP (Dynamic Host Control Protocol) — Protocole fournissant un cadre pour la transmission d'informations relatives à la configuration à des hôtes sur un réseau TCP/IP. Le protocole DHCP se base sur le protocole BOOTP (Bootstrap Protocol), mais propose en outre la possibilité d'une allocation automatique d'adresses réseau réutilisables ainsi que des options de configuration supplémentaires.

Protocole GVRP (GARP VLAN Registration Protocol) — Protocole définissant une méthode permettant aux commutateurs d'échanger des informations sur les VLAN afin d'enregistrer les membres nécessaires des VLAN sur les ports du Spanning Tree de telle sorte que les VLAN définis dans chaque commutateur puissent fonctionner automatiquement via un réseau Spanning Tree.

Regroupement des liaisons — *Voir Groupe de ports*

Remote Authentication Dial-in User Service (RADIUS) — Protocole d'authentification utilisant un serveur central pour contrôler l'accès aux périphériques compatibles RADIUS sur le réseau. Un serveur RADIUS peut être programmé avec une base de données comprenant plusieurs paires nom d'utilisateur/mot de passe avec les niveaux de privilèges associés pour chaque utilisateur ou groupe requérant des droits d'accès à ce commutateur.

Remote Monitoring (RMON) — Fonction proposant une vaste gamme de fonctions de surveillance réseau. RMON élimine les interrogations requises dans le SNMP standard et peut définir des alertes relatives à différents états du trafic, y compris à des types d'erreurs spécifiques.

Réseau local (LAN)	Groupe d'ordinateurs et de périphériques auxiliaires interconnectés.
Réseau local virtuel (VLAN)	Un réseau local virtuel représente un ensemble de noeuds réseau partageant le même domaine de collisions indépendamment de leur emplacement physique ou de leur point de connexion au réseau. Un réseau local virtuel sert de groupe de travail logique sans barrières physiques et permet aux utilisateurs de partager des informations et des ressources comme s'ils étaient situés sur le même LAN.
Segment de liaison	Longueur d'un câble à paire torsadée ou en fibres optiques reliant deux répétiteurs ou un répétiteur à un PC.
Segment LAN	LAN ou domaine de collision distinct.
Simple Network Management Protocol (SNMP)	Protocole d'application de la suite Internet offrant des services de gestion réseau.
Spanning Tree Protocol (STP)	Technologie permettant de rechercher les boucles sur votre réseau. Les boucles apparaissent souvent dans des systèmes de réseau présentant des liaisons compliquées ou des liaisons de sauvegarde. Le Spanning Tree détecte le chemin le plus court possible et y envoie les données, permettant ainsi d'optimiser la performance et l'efficience du réseau.
Station terminale	Station de travail, serveur ou autre périphérique n'agissant pas en tant qu'interconnexion réseau.
Telnet	Structure de communication distante jouant le rôle d'interface avec un périphérique terminal par le biais du protocole TCP/IP.
Terminal Access Controller Access Control System (TACACS)	Protocole d'authentification utilisant un serveur central pour contrôler l'accès aux périphériques compatibles TACACS sur le réseau. Un serveur TACACS peut être programmé avec une base de données comprenant plusieurs paires nom d'utilisateur/mot de passe avec les niveaux de privilèges associés pour chaque utilisateur ou groupe requérant des droits d'accès au commutateur.
Transmission Control Protocol/Internet Protocol (TCP/IP)	Suite de protocoles incluant TCP comme protocole de transfert principal et IP comme protocole de couche réseau.
Trivial File Transfer Protocol (TFTP)	Protocole TCP/IP généralement utilisé pour le téléchargement de logiciels.
Voyant	Diode lumineuse utilisée pour contrôler un périphérique ou un état du réseau.
XModem	Protocole utilisé pour transférer des fichiers entre périphériques. Les données sont regroupées en blocs de 128 octets, et leurs erreurs sont corrigées.

Index

R

S

T

V