

LINKSYS®
Une Division de Cisco Systems, Inc.



Commutateur Ethernet 10/100 8 ports



avec WebView

Guide de l'utilisateur

Modèle N° **SRW208/SRW208G/SRW208L/SRW208P/SRW208MP (EU)**



Copyright et marques commerciales

Les spécifications peuvent être modifiées sans préavis. Linksys est une marque déposée ou une marque commerciale de Cisco Systems, Inc. et/ou de ses filiales aux États-Unis et dans certains autres pays. Copyright © 2006 Cisco Systems, Inc. Tous droits réservés. Les autres noms de marque et de produits sont des marques commerciales, déposées ou non, de leurs détenteurs respectifs.

Comment se servir de ce guide de l'utilisateur

Le guide de l'utilisateur pour les commutateurs WebView a été rédigé pour faciliter au maximum la compréhension des réseaux avec ce commutateur. Les symboles suivants sont contenus dans ce guide de l'utilisateur :



Cette coche indique un élément qui mérite une attention particulière lors de l'utilisation du commutateur.



Ce point d'exclamation vous avertit de dommages possibles à votre commutateur ou à d'autres éléments.



Ce point d'interrogation indique le rappel d'une action que vous êtes susceptible de devoir effectuer pour utiliser votre commutateur.

Outre ces symboles, des définitions concernant des termes techniques sont présentées de la façon suivante :

mot : définition.

De même, chaque figure (diagramme, capture d'écran ou toute autre image) est accompagnée d'un numéro et d'une description, comme ceci :

Figure 0-1 : Exemple de description de figure

Les numéros de figures et les descriptions sont également répertoriés dans la section « Liste des figures ».

Table des matières

Chapitre 1 : Introduction	1
Bienvenue	1
Contenu de ce guide	3
Chapitre 2 : Présentation du commutateur	4
Présentation	4
SRW208 - Panneau avant	4
SRW208G - Panneau avant	5
SRW208L - Panneau avant	7
Modèles SRW208P, SRW208MP - Panneau avant	8
Le panneau arrière	10
Chapitre 3 : Connexion du commutateur	11
Présentation	11
Avant d'installer le commutateur...	12
Choix de positionnement	12
Connexion du commutateur	15
Chapitre 4 : Utilisation de l'interface de la console pour la configuration	16
Présentation	16
Configuration de l'application HyperTerminal	16
Connexion au commutateur par le biais d'une session Telnet	17
Configuration du commutateur à l'aide de l'interface de la console	18
Chapitre 5 : Utilisation de l'utilitaire Web pour la configuration	30
Présentation	30
Méthode d'accès à l'utilitaire Web	30
Onglet Setup - Summary	31
Onglet Setup - Network Settings	32
Onglet Setup - Time	33
Onglet Port Management - Port Settings	34
Onglet Port Management - Link Aggregation	37
Onglet Port Management - LACP	38
Onglet Port Management - PoE Power Settings	39
Onglet VLAN Management - Create VLAN	39
Onglet VLAN Management - Port Settings	40

Onglet VLAN Management - Ports to VLAN	41
Onglet VLAN Management - VLAN to Ports	42
Onglet VLAN Management - GVRP	43
Onglet Statistics - RMON Statistics	43
Onglet Statistics - RMON History	45
Onglet Statistics - RMON Alarm	47
Onglet Statistics - RMON Events	48
Onglet Statistics - Port Utilization	49
Onglet Statistics - 802.1x Statistics	50
Onglet Statistics - GVRP Statistics	50
Onglet ACL - IP Based ACL	51
Onglet ACL - MAC Based ACL	54
Onglet Security - ACL Binding	55
Onglet Security - RADIUS	55
Onglet Security - TACACS+	56
Onglet Security - 802.1x Settings	57
Onglet Security - Port Security	58
Onglet Security - Multiple Hosts	59
Onglet Security - Storm Control	60
QoS (qualité de service)	61
Onglet QoS - CoS Settings	61
Onglet QoS - Queue Settings	62
Onglet QoS - DSCP Settings	63
Onglet QoS - Bandwidth	63
Onglet QoS - Basic Mode	64
Onglet QoS - Advanced Mode	64
Spanning Tree	66
Onglet Spanning Tree - STP Status	67
Onglet Spanning Tree - Global STP	68
Onglet Spanning Tree - STP Port Settings	69
Onglet Spanning Tree - RSTP Port Settings	70
Onglet Spanning Tree - MSTP Properties	72
Onglet Spanning Tree - MSTP Instance Settings	72
Onglet Spanning Tree - MSTP Interface Settings	73
Onglet Multicast - IGMP Snooping	74
Onglet Multicast - Bridge Multicast	76

Onglet Multicast - Bridge Multicast Forward All	77
Onglet SNMP - Global Parameters	77
Onglet SNMP - Views	78
Onglet SNMP - Group Profile	78
Onglet SNMP - Group Membership	80
Onglet SNMP - Communities	81
Onglet SNMP - Notification Filter	82
Onglet SNMP - Notification Recipient	83
Onglet Admin - User Authentication	84
Onglet Admin - Static Address	85
Onglet Admin - Dynamic Address	86
Onglet Admin - Logging	87
Onglet Admin - Port Mirroring	88
Onglet Admin - Cable Test	88
Onglet Admin - Save Configuration	89
Onglet Admin - Firmware Upgrade	90
Onglet Admin - Reboot	90
Onglet Admin - Factory Defaults	91
Onglet Admin - Server Logs	91
Onglet Admin - Memory Logs	92
Onglet Admin - Flash Logs	92
Annexe A : À propos de Gigabit Ethernet et du câblage fibre optique	93
Gigabit Ethernet	93
Câblage fibre optique	93
Annexe B : Aide de Windows	94
Annexe C : Téléchargement à l'aide de Xmodem	95
Procédures du menu Startup	95
Annexe D : Glossaire	97
Annexe E : Spécifications	104
SRW208	104
SRW208G	108
SRW208L	112
SRW208MP	116
SRW208P	120
Annexe F : Garantie	124

Annexe G : Réglementation

125

Annexe H : Contacts

132

Liste des figures

Figure 2-1 : Panneau avant du modèle SRW208	4
Figure 2-2 : Panneau avant du modèle SRW208G	5
Figure 2-3 : Panneau avant du modèle SRW208L	7
Figure 2-4 : Panneau avant du modèle SRW208P	8
Figure 2-5 : Panneau arrière du modèle SSRW208	10
Figure 3-1 : Configuration de réseau type pour le modèle SRW208P	11
Figure 3-2 : Fixation des supports sur le commutateur	13
Figure 3-3 : Montage du commutateur dans la baie	13
Figure 3-4 : Orientation murale correcte (horizontale)	14
Figure 3-5 : Orientation de montage mural incorrecte (verticale)	14
Figure 3-6 : Gabarit de montage mural	14
Figure 4-1 : Recherche de HyperTerminal	16
Figure 4-2 : Description de la connexion	16
Figure 4-3 : Connexion	16
Figure 4-4 : Propriétés de COM1	17
Figure 4-5 : Écran Login de Telnet	17
Figure 4-6 : Switch Main Menu	18
Figure 4-7 : System Configuration Menu	19
Figure 4-8 : Menu System Information	20
Figure 4-9 : Versions	20
Figure 4-10 : General System Information	20
Figure 4-11 : Menu Management Settings	21
Figure 4-12 : Serial Port Configuration	21
Figure 4-13 : Telnet Configuration	21
Figure 4-14 : SSH Configuration	22
Figure 4-15 : SSH Server Configuration	22
Figure 4-16 : SSH Status	22
Figure 4-17 : SSH Crypto Key Generation	23

Figure 4-18 : SSH Keys Fingerprints	23
Figure 4-19 : Username & Password Settings	24
Figure 4-20 : Security Settings	24
Figure 4-21 : SSL Certificate Generation	24
Figure 4-22 : SSL Certificate	25
Figure 4-23 : IP Configuration	25
Figure 4-24 : IP Address Configuration	26
Figure 4-25 : HTTP	26
Figure 4-26 : HTTPS	26
Figure 4-27 : Network Configuration	27
Figure 4-28 : Test Ping	27
Figure 4-29 : Test TraceRoute	27
Figure 4-30 : File Management	28
Figure 4-31 : Restore System Default Settings	28
Figure 4-32 : Reboot System	28
Figure 4-33 : Port Status	29
Figure 4-34 : Port Configuration	29
Figure 5-1 : Écran Login	30
Figure 5-2 : Setup - Summary	31
Figure 5-3 : Setup - Network Settings	32
Figure 5-4 : Setup - Time	33
Figure 5-5 : Port Management - Port Settings	34
Figure 5-6 : Port Settings - Port Configuration Detail	35
Figure 5-7 : Port Management - Link Aggregation	37
Figure 5-8 : Link Aggregation - Link Aggregation Detail	37
Figure 5-9 : Port Management - LACP	38
Figure 5-10 : Port Management - PoE Power Settings	39
Figure 5-11 : VLAN Management - Create VLAN	39
Figure 5-12 : VLAN Management - Port Settings	40
Figure 5-13 : VLAN Management - Ports to VLAN	41

Figure 5-14 : VLAN Management - VLAN to Ports	42
Figure 5-15 : VLAN to Ports - Join VLAN	42
Figure 5-16 : VLAN Management - GVRP	43
Figure 5-17 : Statistics - RMON Statistics	44
Figure 5-18 : Statistics - RMON History	45
Figure 5-19 : Tableau RMON History	46
Figure 5-20 : Statistics - RMON Alarm	47
Figure 5-21 : Statistics - RMON Events	48
Figure 5-22 : RMON Events - Events Log	49
Figure 5-23 : Statistics - Port Utilization	49
Figure 5-24 : Statistics - 802.1x Statistics	50
Figure 5-25 : Statistics - GVRP Statistics	50
Figure 5-26 : ACL - IP Based ACL	52
Figure 5-27 : ACL - Mac Based ACL	54
Figure 5-28 : Security - ACL Binding	55
Figure 5-29 : Security - RADIUS	55
Figure 5-30 : Security - TACACS+	56
Figure 5-31 : Security - 802.1x Settings	57
Figure 5-32 : 802.1x Settings - Setting Timer	57
Figure 5-33 : Security - Port Security	58
Figure 5-34 : Security - Multiple Hosts	60
Figure 5-35 : Security - Storm Control	60
Figure 5-36 : QoS - CoS Settings	61
Figure 5-37 : QoS - Queue Settings	62
Figure 5-38 : QoS - DSCP Settings	63
Figure 5-39 : QoS - Bandwidth	63
Figure 5-40 : QoS - Basic Mode	64
Figure 5-41 : QoS - Advanced Mode	64
Figure 5-42 : Advanced Mode - Out of Profile DSCP	65
Figure 5-43 : Advanced Mode - Policy Name	65

Figure 5-44 : Advanced Mode - New Class Map	65
Figure 5-45 : Advanced Mode - New Aggregate Policer	66
Figure 5-46 : Spanning Tree - STP Status	67
Figure 5-47 : Spanning Tree - Global STP	68
Figure 5-48 : Spanning Tree - STP Port Settings	69
Figure 5-49 : Spanning Tree - RSTP Port Settings	70
Figure 5-50 : Spanning Tree - MSTP Properties	72
Figure 5-51 : Spanning Tree - MSTP Instance Settings	72
Figure 5-52 : Spanning Tree - MSTP Interface Settings	73
Figure 5-53 : Multicast - IGMP Snooping	75
Figure 5-54 : Multicast - Bridge Multicast	76
Figure 5-55 : Multicast - Bridge Multicast Forward All	77
Figure 5-56 : SNMP - Global Parameters	77
Figure 5-57 : SNMP - Views	78
Figure 5-58 : SNMP - Group Profile	79
Figure 5-59 : SNMP - Group Membership	80
Figure 5-60 : SNMP - Communities	81
Figure 5-61 : SNMP - Notification Filter	82
Figure 5-62 : SNMP - Notification Recipient	83
Figure 5-63 : Admin - User Authentication	84
Figure 5-64 : Admin - Static Address	85
Figure 5-65 : Admin - Dynamic Address	85
Figure 5-66 : Admin - Logging	87
Figure 5-67 : Admin - Port Mirroring	88
Figure 5-68 : Admin - Cable Test	88
Figure 5-69 : Admin - Save Configuration	89
Figure 5-70 : Admin - Firmware Upgrade	90
Figure 5-71 : Admin - Reboot	90
Figure 5-72 : Admin - Factory Defaults	91
Figure 5-73 : Admin - Server Logs	91

Figure 5-74 : Admin - Memory Logs	92
Figure 5-75 : Admin - Flash Logs	92
Figure C-1 : Messages d'autoamorçage	95
Figure C-2 : Startup Menu	95
Figure C-3 : Envoyer le fichier	96
Figure C-4 : Téléchargement	96

Chapitre 1 : Introduction

Bienvenue

Ce guide couvre cinq modèles de produits.

- **SRW208** - Commutateur Ethernet 10/100 8 ports avec WebView.
Comporte 8 ports RJ-45 10/100.
- **SRW208G** - Commutateur Ethernet 10/100 8 ports avec WebView et emplacements d'extension.
Comporte 8 ports RJ-45 10/100 et 1 port 10/100/1000 RJ-45 et 1 emplacement MiniGBIC.
- **SRW208L** - Commutateur Ethernet 10/100 8 ports avec WebView et liaison montante 100Base-LX.
Comporte 8 ports RJ-45 10/100 et 1 emplacement MiniGBIC et 1 port pour liaison montante 1 100LX.
- **SRW208MP** - Comporte 8 ports RJ-45 10/100 avec WebView et POE (Power over Ethernet) maximal.
Comporte 8 ports RJ-45 10/100 et 2 ports RJ-45 10/100/1000 et 2 emplacements MiniGBIC partagés.
- **SRW208P** - Commutateur Ethernet 10/100 8 ports avec WebView et POE (Power over Ethernet).
Comporte 8 ports RJ-45 10/100 et 2 ports RJ-45 10/100/1000 et 2 emplacements MiniGBIC partagés.

Pour les besoins de ce manuel, à chaque fois qu'une fonction s'applique à tous les modèles, le numéro de modèle sera cité sous la forme SRW208x. Si un numéro de modèle spécifique est mentionné, la fonction est alors spécifique à ce modèle.

Le commutateur WebView Managed de Linksys vous permet d'agrandir votre réseau en toute sécurité. La configuration du commutateur est sécurisée à l'aide du protocole SSL pour l'accès au Web. Le contrôle de l'utilisateur est sécurisé grâce à la sécurité 802.1x utilisant un mécanisme de notification RADIUS et peut également être contrôlé à l'aide du filtrage basé sur l'adresse MAC.

Les nombreuses fonctions QoS rendent cette solution idéale pour les applications en temps réel telles que les applications voix et vidéo. Les 4 files d'attente de priorité associées à la pondération WRR et aux techniques de répartition selon une priorité stricte facilitent la coexistence efficace du trafic en temps réel et du trafic des données, leur permettant d'atteindre leurs objectifs en matière de QoS. Les utilisateurs individuels ou les applications peuvent se voir attribuer une priorité supérieure à d'autres en utilisant différentes options de classes de services - par port, priorité de couche 2 (802.1p) et priorité de couche 3 (TOS ou DSCP). La diffusion intelligente et le contrôle d'avalanche multidiffusion minimisent et maîtrisent les effets de ces types de trafic sur

le trafic ordinaire. IGMP Snooping limite le trafic vidéo gourmand en bande passante uniquement vers les demandeurs sans inonder les autres utilisateurs. Le trafic entrant peut être contrôlé et le trafic sortant peut être mis en forme en vous permettant de contrôler l'accès au réseau et le débit du trafic.

Il existe des fonctions qui vous permettent d'agrandir et d'étendre votre réseau de commutateurs. L'agrégation de liens permet de configurer plusieurs tronçons de larges bandes passantes entre des commutateurs. Cela augmente également le niveau de fiabilité dans le sens où le système continue à fonctionner si l'un des liens est rompu. Les Spanning Tree (STP), Fast Spanning Tree et Rapid Spanning Tree (RSTP) vous permettent de construire un réseau maillé de commutateurs qui accroît la disponibilité du système.

La riche fonctionnalité de gestion des commutateurs WebView inclut les options de gestion SNMP, RMON, Telnet, et HTTP, ce qui vous permet d'intégrer et de gérer de manière souple ces périphériques dans votre réseau.

Les modèles SRW208P et SRW208MP prennent en charge la détection de charge automatique. Le circuit de commande de l'alimentation détecte automatiquement Power over Ethernet au point d'accès avant de fournir l'alimentation. L'alimentation en énergie d'Ethernet est limitée pour les ports 10/100 Base-T/TX. Le modèle SRW208MP peut fournir une puissance de sortie maximale par port PoE atteignant 15,4 W sur 8 ports simultanément, alors que le modèle SRW208P peut fournir une puissance de sortie maximale sur 4 ports simultanément ou sur 8 ports avec une puissance réduite de moitié.

Contenu de ce guide

Ce guide de l'utilisateur présente les étapes inhérentes à l'installation et à l'utilisation du commutateur.

- **Chapitre 1 : Introduction**
Ce chapitre décrit les applications du commutateur ainsi que le présent guide de l'utilisateur.
- **Chapitre 2 : Présentation du commutateur**
Ce chapitre décrit les caractéristiques physiques du commutateur.
- **Chapitre 3 : Connexion du commutateur**
Ce chapitre explique comment positionner et connecter le commutateur.
- **Chapitre 4 : Utilisation de l'interface de la console pour la configuration**
Ce chapitre vous indique comment utiliser l'interface de la console du commutateur lorsque vous configurez le commutateur.
- **Chapitre 5 : Utilisation de l'utilitaire Web pour la configuration**
Ce chapitre montre comment configurer le commutateur à l'aide de l'utilitaire Web.
- **Annexe A : À propos de Gigabit Ethernet et du câblage fibre optique**
Cette annexe donne une description générale de Gigabit Ethernet et du câblage fibre optique.
- **Annexe B : Aide de Windows**
Cette annexe explique comment utiliser l'aide de Windows pour obtenir des instructions relatives à la mise en réseau, telles que l'installation du protocole TCP/IP.
- **Annexe C : Téléchargement à l'aide de Xmodem**
Cette annexe décrit comment vous pouvez télécharger le logiciel dans le commutateur en utilisant Xmodem.
- **Annexe D : Glossaire**
Cette annexe fournit un glossaire succinct de termes fréquemment utilisés dans le cadre des réseaux.
- **Annexe E : Spécifications**
Cette annexe répertorie les caractéristiques techniques du commutateur.
- **Annexe F : Garantie**
Cette annexe répertorie les informations relatives à la garantie du commutateur.
- **Annexe G : Réglementation**
Cette annexe détaille la réglementation relative au commutateur.
- **Annexe H : Contacts**
Cette annexe fournit des informations sur diverses ressources Linksys que vous pouvez contacter, notamment le support technique.

Chapitre 2 : Présentation du commutateur

Présentation

Les commutateurs diffèrent par le nombre et les types de voyants DEL et de ports. Le panneau avant de chaque commutateur est représenté sur l'une des pages suivantes. Le panneau arrière est le même sur les cinq modèles.

SRW208 - Panneau avant

Les DEL et les ports du commutateur sont situés sur le panneau avant.

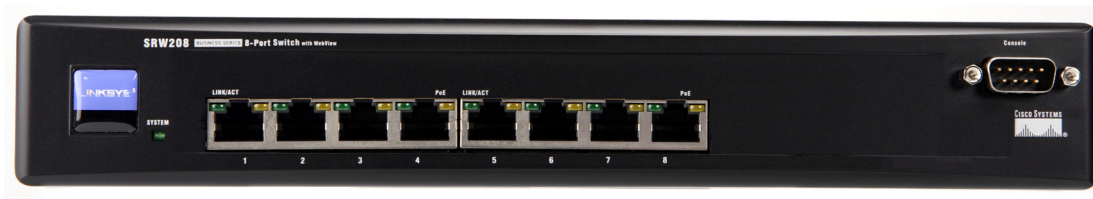


Figure 2-1 : Panneau avant du modèle SRW208

DEL

System	Vert. La DEL SYSTEM s'allume lorsque le commutateur est mis sous tension.
Link/Act	Vert. La DEL LINK/ACT s'allume pour indiquer un lien réseau fonctionnel à travers le port correspondant (1 à 8) avec un périphérique relié. Elle clignote pour indiquer que le commutateur envoie et reçoit des données de manière active à travers ce port.
100M	Orange. La DEL 100M s'allume pour indiquer une connexion à 100 Mbits/s sur le port correspondant (1 à 8).

Ports

1-8 Le commutateur est équipé de 8 ports de réseau Ethernet à détection automatique qui utilisent des connecteurs RJ-45. Les ports Fast Ethernet prennent en charge des vitesses de réseau de 10 ou 100 Mbits/s. Ils peuvent fonctionner en mode semi-duplex et full-duplex. La technologie de détection automatique permet à chaque port de détecter automatiquement la vitesse du périphérique connecté (10 ou 100 Mbits/s) et d'ajuster sa vitesse et la transmission duplex en conséquence.

Console Le port Console est l'emplacement permettant de connecter un câble série au port série d'un ordinateur en vue d'une configuration à l'aide du programme HyperTerminal de votre ordinateur. Reportez-vous au *Chapitre 4 : Utilisation de l'interface de la console pour la configuration* pour plus d'informations.

SRW208G - Panneau avant

Les DEL et les ports du commutateur sont situés sur le panneau avant.



Figure 2-2 : Panneau avant du modèle SRW208G

DEL

System Vert. La DEL **SYSTEM** s'allume lorsque le commutateur est mis sous tension.

Link/Act Vert. La DEL **LINK/ACT** s'allume pour indiquer un lien réseau fonctionnel à travers le port correspondant (1 à 8, G1 ou G2) avec un périphérique relié. Elle clignote pour indiquer que le commutateur envoie et reçoit des données de manière active à travers ce port.

100M Orange. La DEL **100M** s'allume pour indiquer une connexion à 100 Mbits/s sur le port correspondant (1 à 8).

Gigabit Orange. La DEL **Gigabit** s'allume pour indiquer une connexion Gigabit sur le port RJ-45 correspondant (G1) ou sur le port miniGBIC (G2).

Ports

- 1-8** Le commutateur est équipé de 8 ports de réseau Ethernet à détection automatique qui utilisent des connecteurs RJ-45. Les ports Fast Ethernet prennent en charge des vitesses de réseau de 10 ou 100 Mbits/s.
Ils peuvent fonctionner en mode semi-duplex et full-duplex. La technologie de détection automatique permet à chaque port de détecter automatiquement la vitesse du périphérique connecté (10 ou 100 Mbits/s) et d'ajuster sa vitesse et la transmission duplex en conséquence.
- G1** Le port Ethernet Gigabit prend en charge des vitesses de réseau de 10 Mbits/s, 100 Mbits/s et 1 000 Mbits/s. Il peut fonctionner en mode semi-duplex et full-duplex. La technologie de détection automatique permet à chaque port de détecter automatiquement la vitesse du périphérique connecté (10 Mbits/s, 100 Mbits/s ou 1 000 Mbits/s) et d'ajuster sa vitesse et la transmission duplex en conséquence.
- G2** Le port mini-GBIC (convertisseur d'interfaces gigabit) est un point de connexion pour un module d'extension mini-GBIC, ce qui permet la connexion du commutateur à un autre commutateur via une liaison montante par fibre optique. Le port MiniGBIC fournit un lien vers un segment de réseau à haute vitesse ou vers un poste de travail individuel à des vitesses pouvant atteindre 1 000 Mbits/s.
- Utilisez les modules Linksys MGBT1, MGBSX1 ou MGBLH1 mini-GBIC avec le commutateur. Les modules MGBSX1 et MGBLH1 nécessitent un câblage par fibre optique avec les connecteurs LC, alors que le module MGBT1 nécessite un câble Ethernet catégorie 5e avec un connecteur RJ-45.
- Console** Le port Console est l'emplacement permettant de connecter un câble série au port série d'un ordinateur en vue d'une configuration à l'aide du programme HyperTerminal de votre ordinateur. Reportez-vous au *Chapitre 4 : Utilisation de l'interface de la console pour la configuration* pour plus d'informations.

SRW208L - Panneau avant

Les DEL et les ports du commutateur sont situés sur le panneau avant.



Figure 2-3 : Panneau avant du modèle SRW208L

DEL

System	Vert. La DEL SYSTEM s'allume lorsque le commutateur est mis sous tension.
Link/Act	Vert. La DEL LINK/ACT s'allume pour indiquer un lien réseau fonctionnel à travers le port correspondant (1 à 8, G1 ou 100LX) avec un périphérique relié. Elle clignote pour indiquer que le commutateur envoie et reçoit des données de manière active à travers ce port.
100M	Orange. La DEL 100M s'allume pour indiquer une connexion à 100 Mbits/s sur le port correspondant (1 à 8).
Gigabit	Orange. La DEL Gigabit s'allume pour indiquer une connexion Gigabit sur le port RJ-45 (G1) correspondant.

Ports

1-8	<p>Le commutateur est équipé de 8 ports de réseau Ethernet à détection automatique qui utilisent des connecteurs RJ-45. Les ports Fast Ethernet prennent en charge des vitesses de réseau de 10 ou 100 Mbits/s.</p> <p>Ils peuvent fonctionner en mode semi-duplex et full-duplex. La technologie de détection automatique permet à chaque port de détecter automatiquement la vitesse du périphérique connecté (10 ou 100 Mbits/s) et d'ajuster sa vitesse et la transmission duplex en conséquence.</p>
------------	---

- G1** Le port mini-GBIC (convertisseur d'interfaces gigabit) est un point de connexion pour un module d'extension mini-GBIC, ce qui permet la connexion du commutateur à un autre commutateur via une liaison montante par fibre optique. Chaque port MiniGBIC fournit un lien vers un segment de réseau à haute vitesse ou vers un poste de travail individuel à des vitesses pouvant atteindre 1 000 Mbits/s.
- Utilisez les modules Linksys MGBT1, MGBSX1 ou MGBLH1 mini-GBIC avec le commutateur. Les modules MGBSX1 et MGBLH1 nécessitent un câblage par fibre optique avec les connecteurs LC, alors que le module MGBT1 nécessite un câble Ethernet catégorie 5e avec un connecteur RJ-45.
- 9** Le port 100LX est l'emplacement permettant la connexion d'un module 100BASE-LX tel que le module Linksys MFELX1
- Console** Le port Console est l'emplacement permettant de connecter un câble série au port série d'un ordinateur en vue d'une configuration à l'aide du programme HyperTerminal de votre ordinateur. Reportez-vous au *Chapitre 4 : Utilisation de l'interface de la console pour la configuration* pour plus d'informations.

Modèles SRW208P, SRW208MP - Panneau avant

Les DEL et les ports du commutateur sont situés sur le panneau avant.



DEL

- System** Vert. La DEL **SYSTEM** s'allume lorsque le commutateur est mis sous tension.
- Link/Act** Vert. La DEL **LINK/ACT** s'allume pour indiquer un lien réseau fonctionnel à travers le port correspondant (1 à 8) avec un périphérique relié. Elle clignote pour indiquer que le commutateur envoie et reçoit des données de manière active à travers ce port.



REMARQUE : Le modèle SRW208P prend en charge un maximum de 4 ports à 15,4W ou un maximum de 8 ports à 7,5 W. Le modèle SRW208MP prend en charge un maximum de 8 ports à 15,4 W.

PoE Orange. La DEL **PoE** s'allume pour indiquer qu'un périphérique est connecté en utilisant Power over Ethernet sur le port correspondant (1 à 8).

Gigabit Orange. La DEL **Gigabit** s'allume pour indiquer une connexion Gigabit sur le port RJ-45 (G1 à G2) correspondant.

Ports

1-8 Le commutateur est équipé de 8 ports de réseau Ethernet à détection automatique qui utilisent des connecteurs RJ-45. Les ports Fast Ethernet prennent en charge des vitesses de réseau de 10 ou 100 Mbits/s.
Ils peuvent fonctionner en mode semi-duplex et full-duplex. La technologie de détection automatique permet à chaque port de détecter automatiquement la vitesse du périphérique connecté (10 ou 100 Mbits/s) et d'ajuster sa vitesse et la transmission duplex en conséquence.

G1-G2 Les ports Ethernet Gigabit prennent en charge des vitesses de réseau de 10 Mbits/s, 100 Mbits/s et 1 000 Mbits/s. Ils peuvent fonctionner en mode semi-duplex et full-duplex. La technologie de détection automatique permet à chaque port de détecter automatiquement la vitesse du périphérique connecté (10 Mbits/s, 100 Mbits/s ou 1 000 Mbits/s) et d'ajuster sa vitesse et la transmission duplex en conséquence. Les ports RJ-45 G1 et G2 sont partagés avec les ports miniGBIC.

miniGBIC 1/2 Le port mini-GBIC (convertisseur d'interfaces gigabit) est un point de connexion pour un module d'extension mini-GBIC, ce qui permet la connexion du commutateur à un autre commutateur via une liaison montante par fibre optique. Chaque port MiniGBIC fournit un lien vers un segment de réseau à haute vitesse ou vers un poste de travail individuel à des vitesses pouvant atteindre 1 000 Mbits/s.

Utilisez les modules Linksys MGBT1, MGBSX1 ou MGBLH1 mini-GBIC avec le commutateur. Les modules MGBSX1 et MGBLH1 nécessitent un câblage par fibre optique avec les connecteurs LC, alors que le module MGBT1 nécessite un câble Ethernet catégorie 5e avec un connecteur RJ-45.

Console Le port Console est l'emplacement permettant de connecter un câble série au port série d'un ordinateur en vue d'une configuration à l'aide du programme HyperTerminal de votre ordinateur. Reportez-vous au *Chapitre 4 : Utilisation de l'interface de la console pour la configuration* pour plus d'informations.

Le panneau arrière

Le port d'alimentation est situé sur le panneau arrière du commutateur.



Figure 2-5 : Panneau arrière du modèle SSRW208

Power

Le port **Power** est l'emplacement où vous allez brancher le cordon d'alimentation.



REMARQUE : si vous avez besoin de réinitialiser le commutateur, débranchez le cordon d'alimentation à l'arrière du commutateur. Attendez quelques secondes, puis reconnectez-le.

Chapitre 3 : Connexion du commutateur

Présentation

Ce chapitre explique comment connecter des périphériques réseau au commutateur. Pour un exemple de configuration de réseau type, voir le schéma d'application représenté ci-dessous.

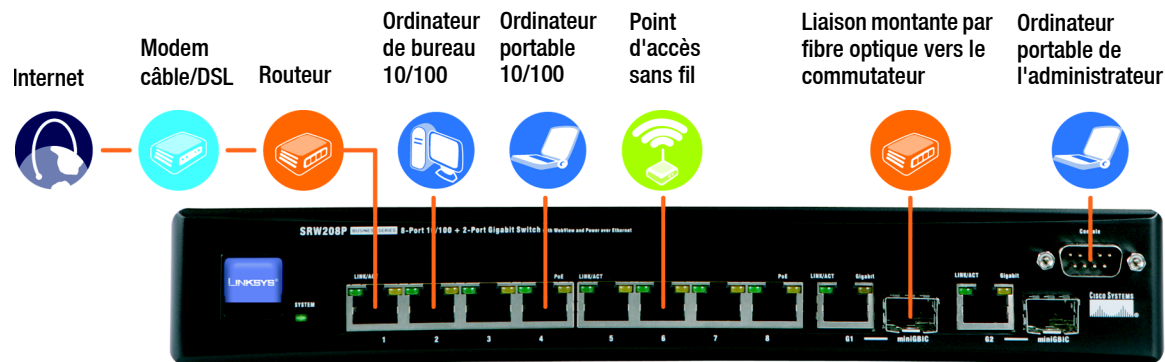


Figure 3-1 : Configuration de réseau type pour le modèle SRW208P

Lorsque vous connectez vos périphériques réseau, assurez-vous qu'ils n'excèdent pas les distances de câblage maximales indiquées dans le tableau suivant :

Tableau 1 : Distances de câblage maximales

De	Vers	Distance maximale
Commutateur	Commutateur ou concentrateur*	100 mètres
Concentrateur	Concentrateur	5 mètres
Commutateur ou concentrateur	Ordinateur	100 mètres

*Un concentrateur fait référence à tout type de concentrateur 100 Mbits/s, y compris les concentrateurs ordinaires et les concentrateurs empilables. Un concentrateur 10 Mbits/s connecté à un autre concentrateur 10 Mbits/s peut couvrir une distance jusqu'à 100 mètres.

Avant d'installer le commutateur...

Lorsque vous choisissez un emplacement pour le commutateur, respectez les règles suivantes :

- Assurez-vous que le commutateur est accessible et que les câbles peuvent être connectés facilement.
- Installez le câblage à distance des sources de parasitage électrique, des lignes d'alimentations et des appareils d'éclairage fluorescent.
- Positionnez le commutateur loin de sources d'eau et d'humidité.
- Pour garantir une circulation d'air adéquate autour du commutateur, assurez-vous de laisser un espace minimal de 50 mm.
- N'empilez pas plus de quatre commutateurs autonomes.

Choix de positionnement

Avant de connecter les câbles au commutateur, vous devez tout d'abord installer physiquement le commutateur. Vous pouvez soit positionner le commutateur sur ses quatre pieds en caoutchouc pour un placement sur un bureau, soit le monter dans une baie de taille standard, de 19 pouces de large et de 1 unité de haut pour un positionnement en baie.

Positionnement sur un bureau

1. Fixez les pieds en caoutchouc sur les zones d'encastrement situées au bas du commutateur.
2. Placez le commutateur sur un bureau à proximité d'une source de courant CA.
3. Laissez un espace de ventilation suffisant pour le commutateur et vérifiez les restrictions relatives à l'environnement mentionnées dans les spécifications.
4. Passez à la section « Connexion du commutateur ».

Positionnement en baie

Pour monter le commutateur dans une baie de taille standard, de 19 pouces de large et de 1 unité de haut, suivez les instructions suivantes :

1. Placez le commutateur sur une surface plane en positionnant le panneau avant en face de vous.
2. Fixez un support de baie sur un côté du commutateur avec les vis fournies. Puis fixez l'autre support sur l'autre côté.
3. Assurez-vous que les supports sont correctement fixés sur le commutateur.
4. Utilisez les vis appropriées (non incluses) pour fixer solidement les supports sur votre baie.

Passez à la section « Connexion du commutateur ».



IMPORTANT : assurez-vous d'utiliser les vis fournies avec les supports de montage. L'utilisation de vis non adaptées pourrait endommager le commutateur et annulerait votre garantie.



Figure 3-2 : Fixation des supports sur le commutateur

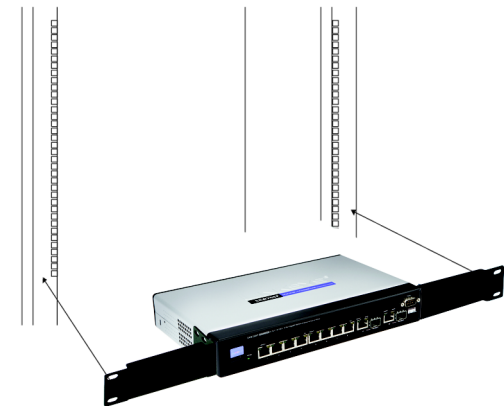


Figure 3-3 : Montage du commutateur dans la baie

Fixation murale

Pour le montage mural du commutateur, ce dernier doit être fixé horizontalement. Le panneau avant doit se trouver soit en haut, soit en bas (voir figure 3-4). L'unité ne doit pas être positionnée verticalement lorsqu'elle est fixée (voir figure 3-5).

Vous aurez besoin de deux vis adaptées pour fixer le commutateur.

1. Déterminez l'endroit où vous souhaitez installer le commutateur. Assurez-vous que le mur que vous utilisez est lisse, plat, sec et robuste et vérifiez que l'emplacement se trouve à portée d'une prise électrique.
2. Percez deux trous dans le mur. Vérifiez que l'entraxe des trous est de 94 mm. Vous pouvez imprimer le gabarit à partir de cette page.
3. Insérez une vis dans chaque trou et laissez leur tête sortir de 3 mm.
4. Positionnez le commutateur de manière à ce que les encoches de montage mural s'alignent avec les deux vis.
5. Placez les encoches de montage mural au-dessus des vis et faites glisser le commutateur vers le bas jusqu'à ce que les vis s'insèrent parfaitement dans les encoches de montage mural.

Félicitations ! L'installation murale du commutateur est terminée.

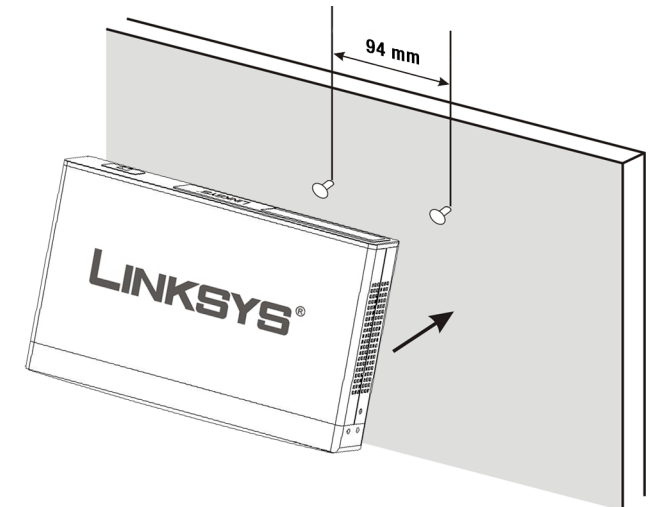


Figure 3-4 : Orientation murale correcte (horizontale)



IMPORTANT : pour la fixation murale, veillez à ce que le commutateur soit installé horizontalement. N'installez pas le commutateur verticalement.

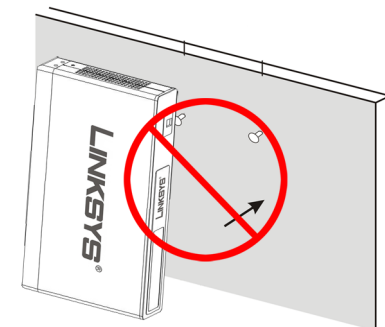
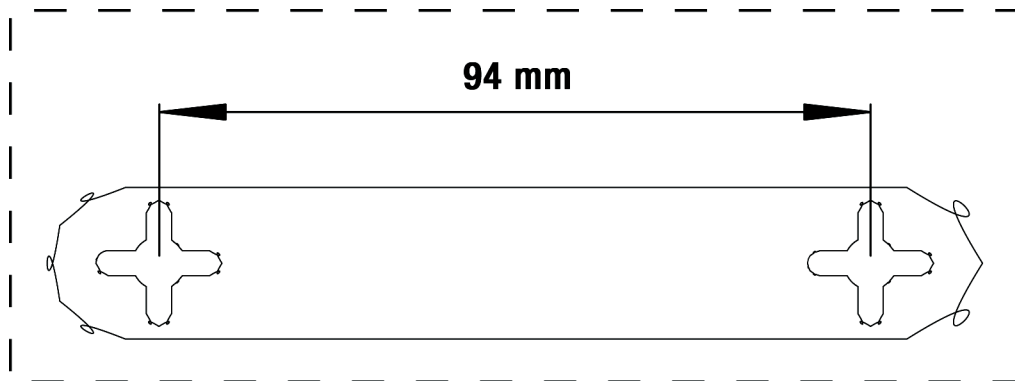


Figure 3-5 : Orientation de montage mural incorrecte (verticale)



Imprimez cette page à une échelle de 100 %, coupez le long de la ligne en pointillés et placez-la sur le mur pour effectuer le perçage avec un espacement précis.

Figure 3-6 : Gabarit de montage mural

Connexion du commutateur

Pour connecter des périphériques réseau au commutateur, suivez les instructions suivantes :

1. Assurez-vous que tous les périphériques que vous allez connecter au commutateur sont hors tension.
2. Pour les périphériques 10/100 Mbps/s, connectez un câble réseau Ethernet de catégorie 5 à l'un des ports numérotés sur le commutateur. Pour un périphérique 1 000 Mbps/s, connectez un câble réseau Ethernet de catégorie 5e à l'un des ports numérotés sur le commutateur.
3. Connectez l'autre extrémité à un ordinateur ou à un autre périphérique réseau.
4. Répétez les étapes 2 et 3 pour connecter des périphériques supplémentaires.
5. Si vous utilisez le port mini-GBIC, connectez alors le module mini-GBIC au port mini-GBIC. Pour des instructions détaillées, reportez-vous à la documentation du module.
6. Si vous utilisez l'interface de la console du commutateur pour configurer le commutateur, connectez alors le câble série fourni au port de la console du commutateur et serrez les vis de fixation imperdables. Connectez l'autre extrémité au port série de votre ordinateur (cet ordinateur doit exécuter le logiciel d'émulation du terminal VT100, tel que HyperTerminal).
7. Branchez le cordon d'alimentation fourni au port d'alimentation du connecteur, puis branchez l'autre extrémité à une prise électrique.



IMPORTANT : assurez-vous d'utiliser le cordon d'alimentation fourni avec le commutateur. L'utilisation d'un cordon d'alimentation différent pourrait endommager le commutateur.



REMARQUE : si vous avez besoin de réinitialiser le commutateur, débranchez le cordon d'alimentation à l'arrière du commutateur. Attendez quelques secondes, puis reconnectez-le.

8. Mettez sous tension les périphériques réseau connectés au commutateur. Chaque DEL Link/Act du port actif correspondant va s'allumer sur le commutateur. Si un port dispose d'une connexion Gigabit active, sa DEL Gigabit correspondante va également s'allumer.

Si vous utilisez l'interface de la console du commutateur pour configurer le commutateur, passez au Chapitre 4 : Utilisation de l'interface de la console pour la configuration pour de plus amples instructions.

Si vous utilisez l'utilitaire Web du commutateur pour configurer le commutateur, passez au Chapitre 5 : Utilisation de l'utilitaire Web pour la configuration.

Chapitre 4 : Utilisation de l'interface de la console pour la configuration

Présentation

Le commutateur comporte une interface de console pilotée par menu pour une configuration de base du commutateur et la gestion de votre réseau. Le commutateur peut être configuré en utilisant CLI par le biais de l'interface de la console ou via une connexion telnet. Ce chapitre décrit la configuration de l'interface de la console. La configuration peut également être effectuée grâce à l'utilitaire Web, ce qui est traité dans le chapitre suivant.

Configuration de l'application HyperTerminal

Avant d'utiliser l'interface de la console, vous aurez besoin de configurer l'application HyperTerminal sur votre ordinateur.

1. Cliquez sur le bouton **Démarrer**. Sélectionnez **Programmes** puis **Accessoires**. Sélectionnez **Communications**. Sélectionnez **HyperTerminal** dans les options proposées dans ce menu.
2. Dans l'écran *Description de la connexion*, saisissez un nom pour cette connexion. Dans l'exemple, le nom de la connexion est SRW208. Sélectionnez une icône pour l'application. Cliquez ensuite sur le bouton **OK**.
3. Dans l'écran *Connexion*, sélectionnez un port pour communiquer avec le commutateur : **COM1**, **COM2** ou **TCP/IP**.

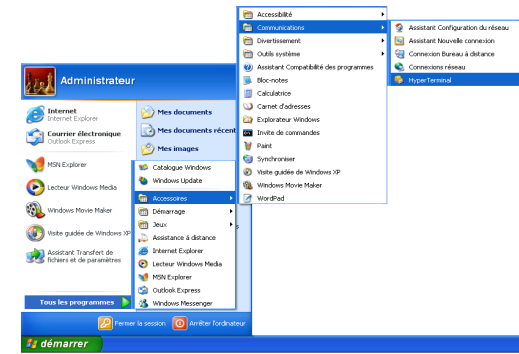


Figure 4-1 : Recherche de HyperTerminal



Figure 4-2 : Description de la connexion



Figure 4-3 : Connexion

4. Définissez les paramètres du port série de la façon suivante :

Bits par seconde : **38400**

Bits de données : **8**

Parité : **Aucun**

Bits d'arrêt : **1**

Contrôle de flux : **Aucun**

Cliquez ensuite sur le bouton **OK**.

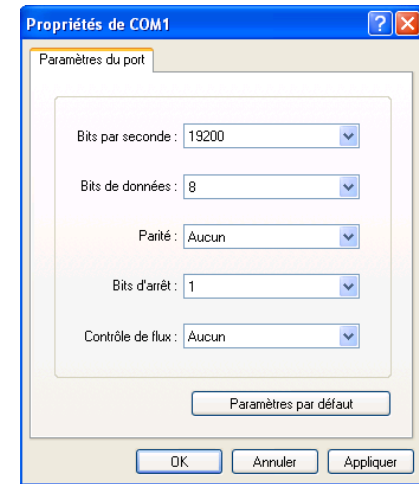


Figure 4-4 : Propriétés de COM1

Connexion au commutateur par le biais d'une session Telnet

Ouvrez un éditeur de ligne de commande et saisissez **telnet 192.168.1.254**. Appuyez ensuite sur la touche **Entrée**.

L'écran *Login* va alors apparaître. La première fois que vous ouvrez l'interface CLI, sélectionnez **Edit** et appuyez sur **Entrée**. Saisissez **admin** dans le champ *User Name*. Laissez le champ *Password* vierge.

Appuyez sur le bouton **Echap** et vous retournerez à l'écran de connexion. Appuyez sur le bouton flèche droite pour naviguer jusqu'à **Execute** puis sur le bouton **Entrée** pour accéder à l'interface CLI.

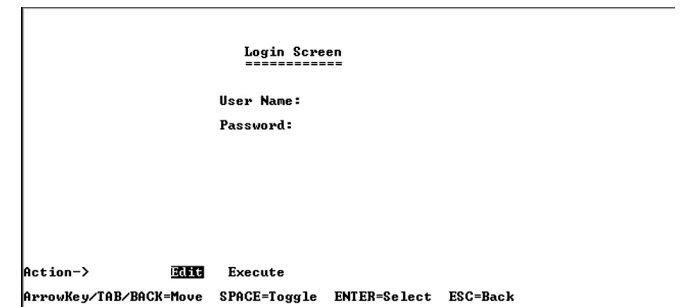


Figure 4-5 : Écran Login de Telnet

Configuration du commutateur à l'aide de l'interface de la console

Les écrans de la console se composent d'un ensemble de menus. Chaque menu possède plusieurs options, qui sont présentées verticalement. Vous sélectionnez une option de menu lorsque vous la mettez en surbrillance ; un appui sur la touche **Entrée** active l'option de surbrillance.

Pour naviguer à travers les menus et les actions de l'interface de la console, utilisez les touches flèches vers le haut et vers le bas pour vous déplacer vers le haut ou vers le bas, et utilisez les touches flèche vers la gauche ou vers la droite pour vous déplacer à gauche ou à droite. Utilisez la touche Entrée pour sélectionner une option du menu et la touche Echap pour revenir à la sélection précédente. Les options de menu et toutes les valeurs saisies ou présentes seront mises en surbrillance. Au bas de l'écran figure une liste des actions disponibles.

Switch Main Menu

L'écran *Switch Main Menu* affiche les choix suivants :

1. System Configuration Menu
2. Port Status
3. Port Configuration
4. Help
0. Logout

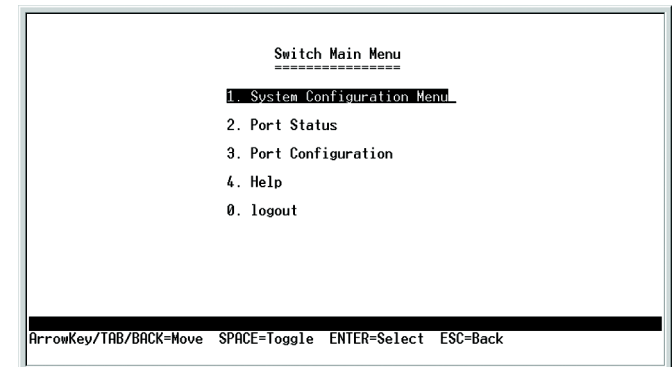


Figure 4-6 : Switch Main Menu

System Configuration Menu

Dans l'écran *System Configuration Menu* , vous disposez des choix suivants :

1. System Information
2. Management Settings
3. User & Password Settings
4. Security Settings
5. IP Configuration
6. File Management
7. Restore System Default Settings
8. Reboot System
0. Back to main menu

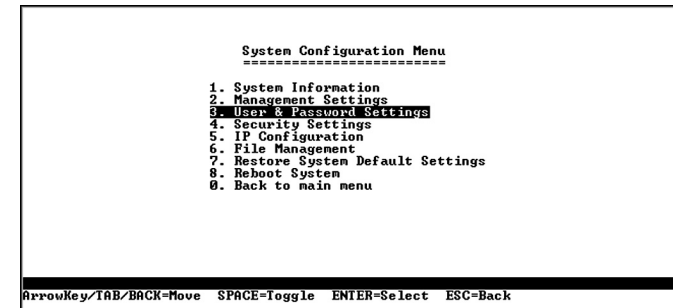


Figure 4-7 : System Configuration Menu

System Information

En utilisant cet écran, vous pouvez vérifier les versions du micrologiciel du commutateur et obtenir des informations générales sur le système.

Versions

L'écran *Versions* affiche les versions d'amorçage, du logiciel et du micrologiciel du matériel du commutateur.

General System Information

L'écran *General System Information* affiche les informations suivantes : System Description, System Up Time, System MAC Address, System Contact, System Name et System Location.

Sélectionnez **Edit** et appuyez sur la touche **Entrée** pour effectuer les modifications. Une fois vos modifications effectuées, appuyez sur la touche **Echap** pour revenir au menu *Action*. Sélectionnez **Save** et appuyez sur la touche **Entrée** pour enregistrer vos modifications. Pour quitter cet écran, sélectionnez **Quit** et appuyez sur la touche **Entrée**.

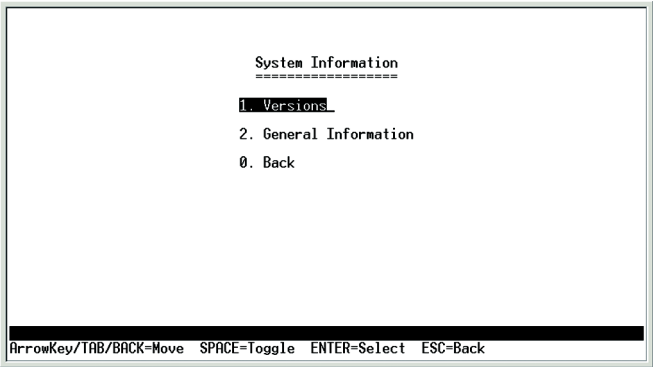


Figure 4-8 : Menu System Information

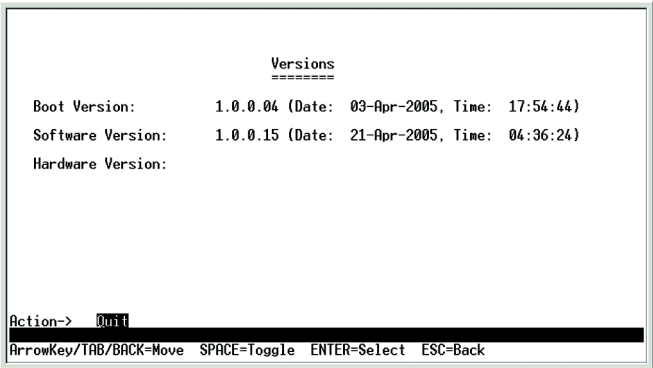


Figure 4-9 : Versions

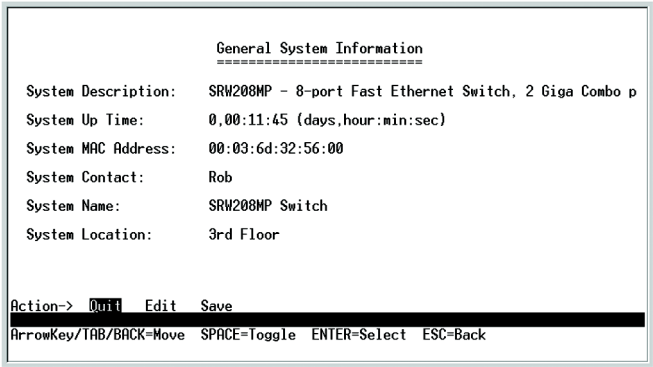


Figure 4-10 : General System Information

Management Settings

À partir de l'écran Management Settings, vous pouvez définir les configurations suivantes : Serial Port Session Configuration, Telnet Session Configuration ou Secure Telnet (SSH) Configuration.

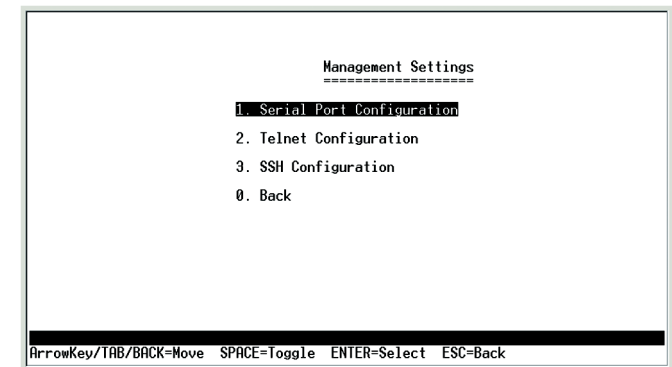


Figure 4-11 : Menu Management Settings

Serial Port Configuration

Dans l'écran *Serial Port Configuration* le débit en bauds du commutateur est affiché.

Sélectionnez **Edit** et appuyez sur la touche **Entrée** pour effectuer les modifications. Basculez vers la vitesse désirée et, une fois vos modifications effectuées, appuyez sur la touche **Echap** pour revenir au menu *Action*. Sélectionnez **Save** et appuyez sur la touche **Entrée** pour enregistrer vos modifications. Pour quitter cet écran, sélectionnez **Quit** et appuyez sur la touche **Entrée**.

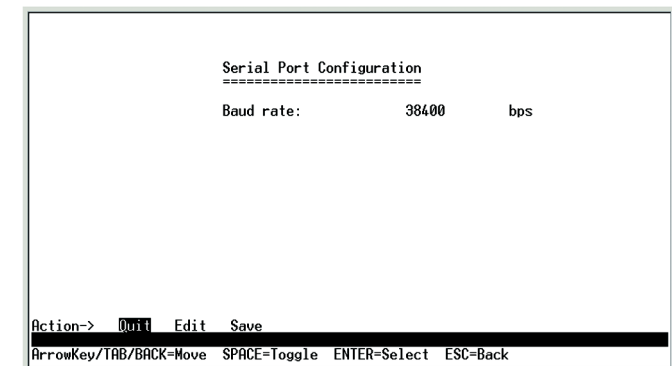


Figure 4-12 : Serial Port Configuration

Telnet Configuration

Sur l'écran *Telnet Configuration*, le délai est affiché. La valeur est entrée en secondes. Si vous ne voulez pas de délai pour la session Telnet, vous pouvez entrer une valeur de 0 seconde.

Sélectionnez **Edit** et appuyez sur la touche **Entrée** pour effectuer les modifications. Une fois vos modifications effectuées, appuyez sur la touche **Echap** pour revenir au menu *Action*. Sélectionnez **Save** et appuyez sur la touche **Entrée** pour enregistrer vos modifications. Pour quitter cet écran, sélectionnez **Quit** et appuyez sur la touche **Entrée**.

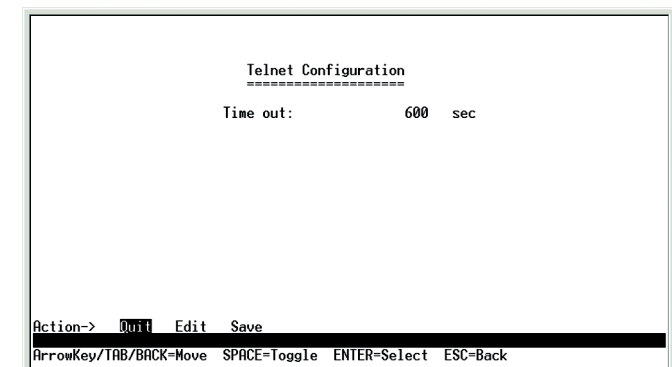


Figure 4-13 : Telnet Configuration

SSH Configuration

Sur l'écran SSH Configuration, vous pouvez sélectionner l'une des options suivantes : SSH Server Configuration, SSH Server Status, SSH Crypto Key Generation et SSH Keys Fingerprints.

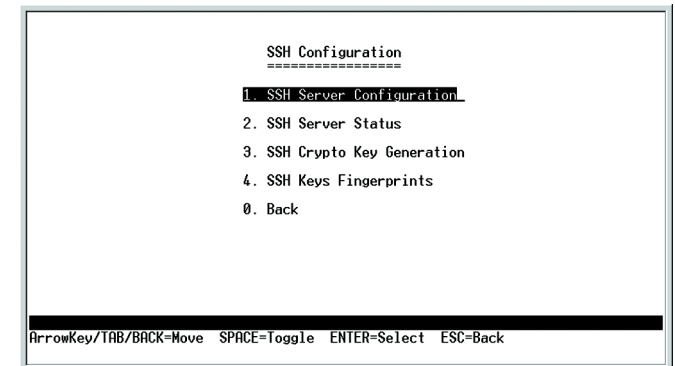


Figure 4-14 : SSH Configuration

SSH Server Configuration

Sur l'écran *SSH Server Configuration*, le serveur SSH peut être activé ou désactivé en naviguant vers l'option du serveur SSH et en utilisant la barre **ESPACE** pour changer d'option. Le port du serveur SSH peut être modifié en saisissant une valeur.

Sélectionnez **Edit** et appuyez sur la touche **Entrée** pour effectuer les modifications. Une fois vos modifications effectuées, appuyez sur la touche **Echap** pour revenir au menu *Action*. Sélectionnez **Save** et appuyez sur la touche **Entrée** pour enregistrer vos modifications. Pour quitter cet écran, sélectionnez **Quit** et appuyez sur la touche **Entrée**.

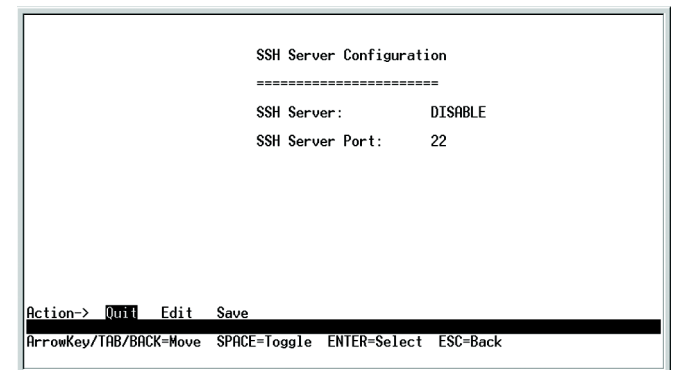


Figure 4-15 : SSH Server Configuration

SSH Status

L'écran *SSH Status* affiche si le serveur SSH est activé, l'état de la clé RSA et DSA ainsi que toute session SSH ouverte.

Sélectionnez **Refresh** pour mettre à jour l'écran si nécessaire. Pour quitter cet écran, sélectionnez **Quit** et appuyez sur la touche **Entrée**.

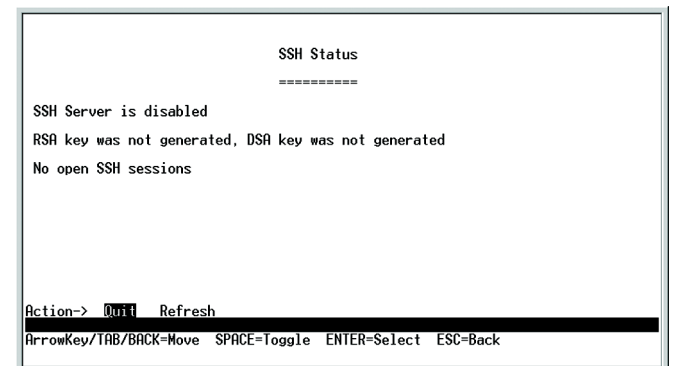


Figure 4-16 : SSH Status

SSH Crypto Key Generation

Sur l'écran *SSH Crypto Key Generation*, l'algorithme de clé publique SSH peut être basculé entre RSA et DSA à l'aide de la barre **ESPACE**. Il n'est pas possible de modifier la longueur de la clé publique SSH.

Sélectionnez **Edit** et appuyez sur la touche **Entrée** pour effectuer les modifications. Une fois vos modifications effectuées, appuyez sur la touche **Echap** pour revenir au menu *Action*. Sélectionnez **Save** et appuyez sur la touche **Entrée** pour enregistrer vos modifications. Pour quitter cet écran, sélectionnez **Quit** et appuyez sur la touche **Entrée**.

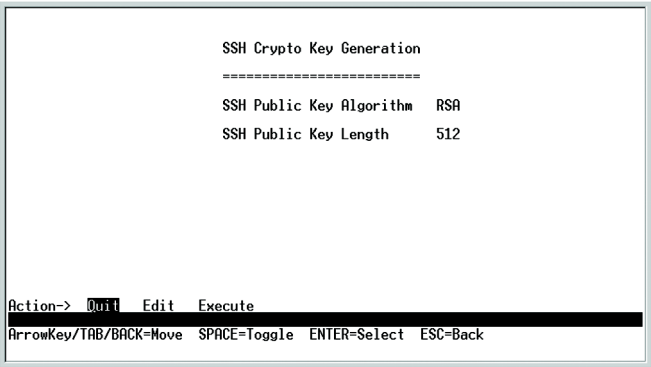


Figure 4-17 : SSH Crypto Key Generation

SSH Keys Fingerprints

Dans l'écran *SSH Keys Fingerprints*, les clés RSA et DSA seront affichées si elles ont été générées.

Sélectionnez **Refresh** pour mettre à jour l'écran si nécessaire. Pour quitter cet écran, sélectionnez **Quit** et appuyez sur la touche **Entrée**.

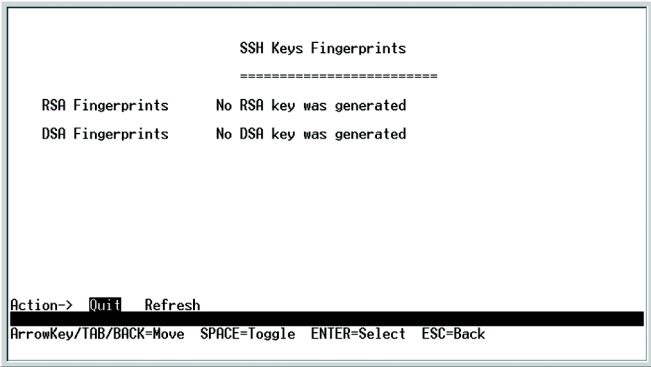


Figure 4-18 : SSH Keys Fingerprints

Username & Password Settings

À partir de cet écran, vous pouvez administrer les noms d'utilisateur et les mots de passe des personnes qui accèdent au commutateur.

Sélectionnez **Edit** et appuyez sur la touche **Entrée** pour effectuer les modifications. Une fois vos modifications effectuées, appuyez sur la touche **Echap** pour revenir au menu *Action*. Sélectionnez **Save** et appuyez sur la touche **Entrée** pour enregistrer vos modifications. Pour quitter cet écran, sélectionnez **Quit** et appuyez sur la touche **Entrée**.



REMARQUE : l'écran Username & Password Settings peut également être utilisé pour définir des mots de passe pour d'autres utilisateurs.

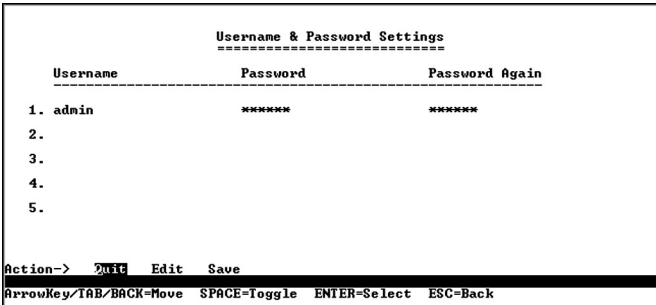


Figure 4-19 : Username & Password Settings

Security Settings

L'écran Security Settings vous permet de configurer les paramètres de sécurité du commutateur, ainsi que de générer et d'afficher le certificat.



Figure 4-20 : Security Settings

SSL Certificate Generation

Utilisez l'écran SSL Certificate Generation pour spécifier un certificat généré par le périphérique.

Les champ suivants sont spécifiés :

Public Key Length : indique la longueur de la clé RSA SSL (Plage : 512 - 2048).

Organization Name : indique le nom de l'organisation (Plage : 1 - 64).

Locality or City Name : indique le nom de l'emplacement ou de la ville (Plage : 1 - 64).

State or Province Name : indique le nom de l'état ou de la province (Plage : 1 - 64).

Country Name : indique le nom du pays (Plage : 2 - 2).

Validity Term : indique le nombre de jours pendant lesquels la certification est valide (Plage : 30 - 3650).

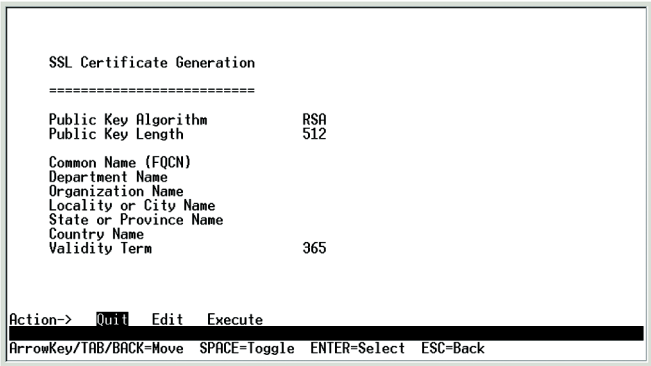


Figure 4-21 : SSL Certificate Generation

Show Certificate

Utilisez l'écran Show Certificate pour afficher le certificat interne.

```
SSL Certificate
=====
Issued by : C= , ST= , L= , CN=0.0.0.0, O= , OU=
Valid From: Jan 1 01:14:30 2000 GMT
Valid to: Dec 31 01:14:30 2000 GMT
Subject: C= , ST= , L= , CN=0.0.0.0, O= , OU=
Fingerprint: 044BD9A6 48984CAC EBF05632 FB6E987B D71B61CE

Action-> Quit Refresh
ArrowKey/TAB/BACK=Move SPACE=Toggle ENTER=Select ESC=Back
```

Figure 4-22 : SSL Certificate

Disable Active Management Access Profile

Lors de la sélection de cette option, il vous sera demandé de confirmer que vous souhaitez désactiver le profil de gestion actif.

```
Security Settings
=====
1. SSL Generate Certificate
2. SSL Show Certificate
3. Disable Active Management Access Profile
0. Back

Are you sure? [Y/N]?
ArrowKey/TAB/BACK=Move SPACE=Toggle ENTER=Select ESC=Back
```

IP Configuration

L'écran *IP Configuration* affiche les choix suivants : IP Address Settings, HTTP Configuration, HTTPS Configuration et Network Configuration.

```
IP Configuration
=====
1. IP Address Settings
2. HTTP Configuration
3. HTTPS Configuration
4. Network Configuration
0. Back

ArrowKey/TAB/BACK=Move SPACE=Toggle ENTER=Select ESC=Back
```

Figure 4-23 : IP Configuration

IP Address Configuration

Les informations IP du commutateur s'affichent ici.

IP Address. L'adresse IP du commutateur est affichée (l'adresse IP par défaut est **192.168.1.254**). Vérifiez que l'adresse que vous entrez est correcte et ne provoque pas de conflit avec un autre périphérique sur le réseau.

Subnet Mask. Le masque de sous-réseau du commutateur est affiché.

Default Gateway. L'adresse IP de la passerelle par défaut de votre réseau est affichée.

Management VLAN. Le numéro d'identification du réseau VLAN est affiché.

DHCP client. L'état du client DHCP est affiché. Si vous souhaitez que le commutateur soit un client DHCP, sélectionnez alors **ENABLE**. Si vous souhaitez affecter une adresse IP statique au commutateur, entrez alors les paramètres IP et sélectionnez **DISABLE**.

Sélectionnez **Edit** pour effectuer les modifications. Une fois vos modifications effectuées, appuyez sur la touche **Echap** pour revenir au menu **Action** et sélectionnez **Save** pour enregistrer vos modifications.

HTTP

L'écran *HTTP* affiche l'état et le numéro de port du serveur HTTP.

Sélectionnez **Edit** et appuyez sur la touche **Entrée** pour effectuer les modifications. Une fois vos modifications effectuées, appuyez sur la touche **Echap** pour revenir au menu **Action**. Sélectionnez **Save** et appuyez sur la touche **Entrée** pour enregistrer vos modifications. Pour quitter cet écran, sélectionnez **Quit** et appuyez sur la touche **Entrée**.

HTTPS

Utilisez l'écran *HTTPS* pour configurer les paramètres du protocole HTTPS. Vous pouvez activer ou désactiver le serveur HTTPS et configurer le port sur lequel la session est activée.

Sélectionnez **Edit** et appuyez sur la touche **Entrée** pour effectuer les modifications. Une fois vos modifications effectuées, appuyez sur la touche **Echap** pour revenir au menu **Action**. Sélectionnez **Save** et appuyez sur la touche **Entrée** pour enregistrer vos modifications. Pour quitter cet écran, sélectionnez **Quit** et appuyez sur la touche **Entrée**.

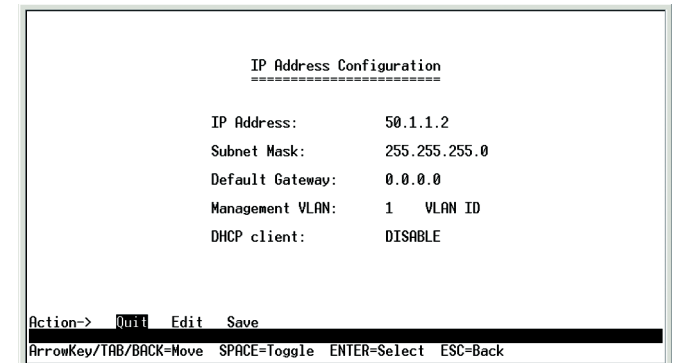


Figure 4-24 : IP Address Configuration

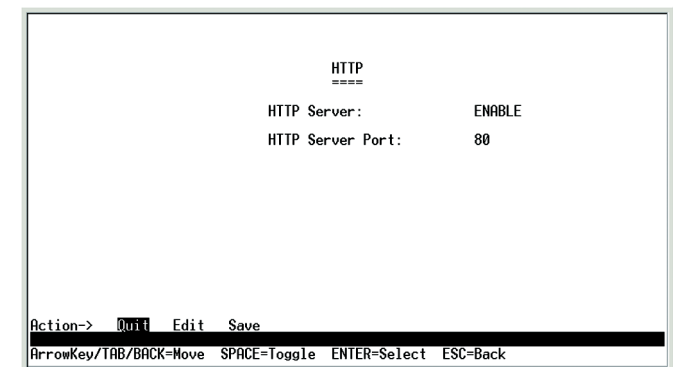


Figure 4-25 : HTTP

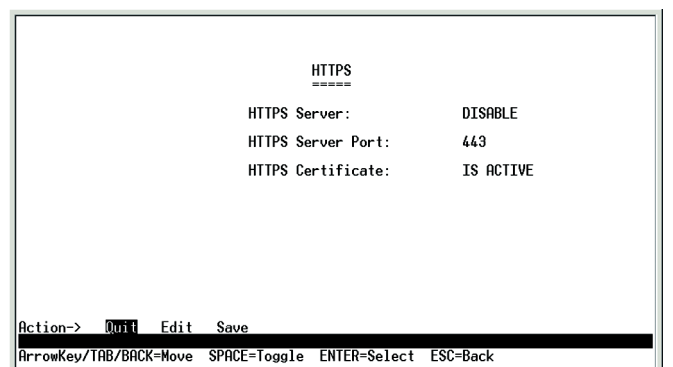


Figure 4-26 : HTTPS

Network Configuration

L'écran *Network Configuration* permet de choisir entre deux tests, Ping et TraceRoute.

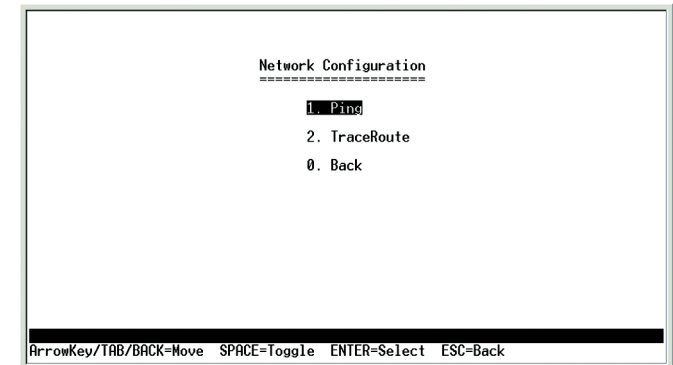


Figure 4-27 : Network Configuration

Ping

L'écran *Ping* affiche l'adresse IP de l'emplacement que vous souhaitez contacter.

Sélectionnez **Edit** pour modifier l'adresse IP et **Execute** pour commencer le test ping.

Une fois le test ping terminé, l'écran *Ping* affiche l'adresse IP, l'état et les statistiques relatives au test ping.

Sélectionnez **Edit** et appuyez sur la touche **Entrée** pour effectuer les modifications. Une fois vos modifications effectuées, appuyez sur la touche **Echap** pour revenir au menu *Action*. Sélectionnez **Save** et appuyez sur la touche **Entrée** pour enregistrer vos modifications. Pour quitter cet écran, sélectionnez **Quit** et appuyez sur la touche **Entrée**.

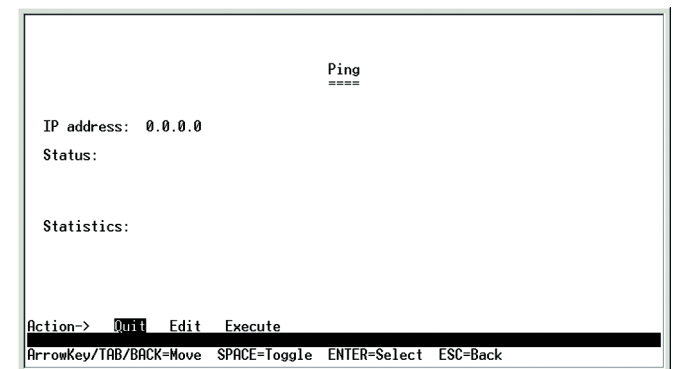


Figure 4-28 : Test Ping

TraceRoute

L'écran *TraceRoute* affiche l'adresse IP de l'adresse de la route que vous souhaitez repérer.

Sélectionnez **Edit** pour modifier l'adresse IP, et sélectionnez **Execute** pour commencer le test traceroute.

Une fois le test traceroute terminé, l'écran *TraceRoute* affiche l'adresse IP, l'état et les statistiques relatives au test traceroute.

Sélectionnez **Edit** et appuyez sur la touche **Entrée** pour effectuer les modifications. Une fois vos modifications effectuées, appuyez sur la touche **Echap** pour revenir au menu *Action*. Sélectionnez **Save** et appuyez sur la touche **Entrée** pour enregistrer vos modifications. Pour quitter cet écran, sélectionnez **Quit** et appuyez sur la touche **Entrée**.

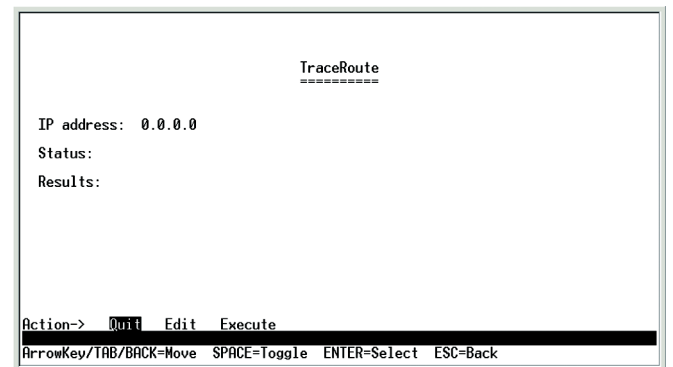


Figure 4-29 : Test TraceRoute

File Management

L'écran *File Management* vous permet de télécharger des fichiers dans le sens montant ou descendant, tels que la configuration de démarrage, l'amorçage ou un fichier image, à l'aide d'un serveur TFTP.

Sélectionnez **Edit** pour effectuer les modifications. Une fois vos modifications effectuées, appuyez sur la touche **Echap** pour revenir au menu *Action* et sélectionnez **Execute** pour télécharger les fichiers souhaités. Une fois que vous avez téléchargé un nouveau fichier image, vous devez redémarrer le périphérique.

Si vous téléchargez une nouvelle image d'amorçage, veuillez procéder comme suit :

1. Téléchargez le nouveau code d'amorçage. NE RÉINITIALISEZ PAS LE PÉRIPHÉRIQUE !
2. Téléchargez la nouvelle image logicielle.
3. Réinitialisez maintenant le périphérique.



REMARQUE : lorsque vous téléchargez un fichier de configuration, vérifiez qu'il s'agit d'un fichier de configuration valide. Si vous avez modifié le fichier, assurez-vous que seules des entrées valides ont été configurées.

Restore System Default Settings

Pour restaurer le commutateur aux paramètres d'usine par défaut, sélectionnez **Restore System Default Settings** et appuyez sur la touche **Entrée**. Il vous sera demandé si vous souhaitez continuer. Appuyez sur la touche **y** pour restaurer les paramètres par défaut du commutateur ou sur la touche **n** pour annuler.

Reboot System

Sélectionnez **Reboot System** puis appuyez sur la touche **Entrée** si vous souhaitez redémarrer le commutateur. Il vous sera demandé si vous souhaitez continuer. Appuyez sur la touche **y** pour redémarrer le commutateur ou sur la touche **n** pour annuler. Une fois que le commutateur a redémarré, l'écran *Switch Main Menu* s'affiche.

Back to main menu

Sélectionnez **Back to main menu** puis appuyez sur la touche **Entrée** si vous souhaitez revenir à l'écran *Switch Main Menu*.

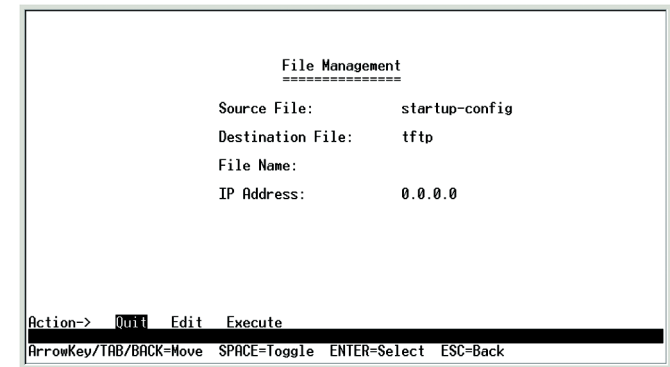


Figure 4-30 : File Management

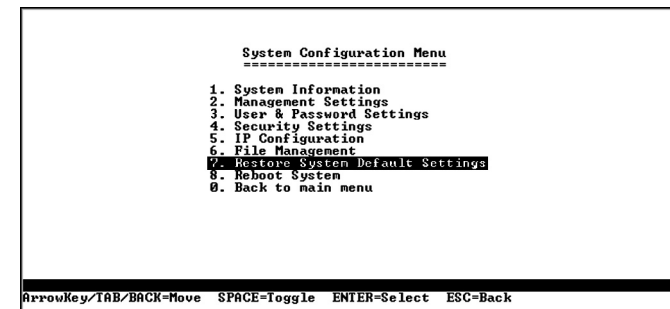


Figure 4-31 : Restore System Default Settings

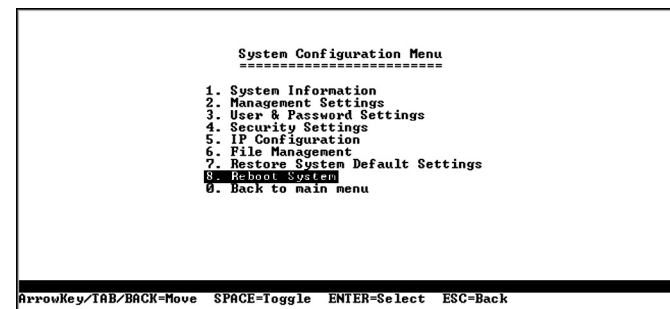


Figure 4-32 : Reboot System

Port Status

Dans l'écran *Switch Main Menu*, sélectionnez **Port Status** puis appuyez sur la touche **Entrée** si vous souhaitez afficher des informations sur l'état des ports du commutateur.

L'écran *Port Status* affiche les numéros des ports, leur état, l'état des liens, la vitesse et le mode duplex ainsi que l'état du contrôle de flux, qui représente le débit des transmissions de paquets.

Si vous souhaitez modifier un paramètre d'un port, vous devez utiliser l'écran *Port Configuration*.

Port Status				
Port	Enable	Link	Spd/Dpx	Flow Ctrl
FAST1	ENABLE	DOWN	-----	---
FAST2	ENABLE	DOWN	-----	---
FAST3	ENABLE	UP	100F	Off
FAST4	ENABLE	DOWN	-----	---
FAST5	ENABLE	DOWN	-----	---
FAST6	ENABLE	DOWN	-----	---
FAST7	ENABLE	DOWN	-----	---
FAST8	ENABLE	DOWN	-----	---
GIGA1	ENABLE	DOWN	-----	---
GIGA2	ENABLE	DOWN	-----	---
Action-> Quit Refresh				
ArrowKey/TAB/BACK=Move SPACE=Toggle ENTER=Select ESC=Back				

Figure 4-33 : Port Status

Port Configuration

Dans l'écran *Switch Main Menu*, sélectionnez **Port Configuration** puis appuyez sur la touche **Entrée** si vous souhaitez configurer les ports du commutateur.

L'écran *Port Configuration* affiche les numéros des ports, leur état, l'état de la négociation automatique, la vitesse et le mode duplex ainsi que l'état du contrôle de flux, qui représente le débit des transmissions de paquets.

Sélectionnez **Edit** et appuyez sur la touche **Entrée** pour effectuer les modifications. Une fois vos modifications effectuées, appuyez sur la touche **Echap** pour revenir au menu *Action*. Sélectionnez **Save** et appuyez sur la touche **Entrée** pour enregistrer vos modifications. Pour quitter cet écran, sélectionnez **Quit** et appuyez sur la touche **Entrée**.

Port Configuration				
Port	Enable	Auto Neg.	Spd/Dpx	Flow Ctrl
FAST1	ENABLE	On	Auto	Off
FAST2	ENABLE	On	Auto	Off
FAST3	ENABLE	On	Auto	Off
FAST4	ENABLE	On	Auto	Off
FAST5	ENABLE	On	Auto	Off
FAST6	ENABLE	On	Auto	Off
FAST7	ENABLE	On	Auto	Off
FAST8	ENABLE	On	Auto	Off
GIGA1	ENABLE	On	Auto	Off
GIGA2	ENABLE	On	Auto	Off
Action-> Quit Edit Save				
ArrowKey/TAB/BACK=Move SPACE=Toggle ENTER=Select ESC=Back				

Figure 4-34 : Port Configuration

Help

Sélectionnez **Help** et appuyez sur la touche **Entrée** si vous souhaitez afficher les informations d'aide. Cet écran explique comment naviguer dans les différents écrans de l'interface de la console.

Chapitre 5 : Utilisation de l'utilitaire Web pour la configuration

Présentation

Ce chapitre est un guide de référence détaillé de l'utilitaire Web. Toutes les fonctions présentées dans ce chapitre sont incluses dans les commutateurs Fast Ethernet, sauf mention contraire. Les fonctions propres à des commutateurs spécifiques sont signalées.

Méthode d'accès à l'utilitaire Web



REMARQUE : l'utilitaire Web est optimisé pour l'affichage d'une résolution d'écran de 1024 x 768. Internet Explorer version 5.5 ou ultérieure est recommandé.

Ouvrez votre navigateur Web et entrez **192.168.1.1** dans le champ *Address*. Appuyez sur la touche **Entrée**. L'écran d'ouverture de session apparaît.



REMARQUE : l'adresse IP par défaut du périphérique est 192.168.1.254. Si vous avez modifié cette adresse, entrez l'adresse IP correcte. Le périphérique doit se trouver sur le même sous-réseau que la station de gestion utilisée pour configurer le périphérique.

Lors de votre première utilisation de l'utilitaire Web, entrez **admin** dans le champ *User Name* et laissez le champ *Password* vide. Cliquez sur le bouton **OK**. Vous pourrez ultérieurement définir un mot de passe dans l'écran *System Password*.

Le premier écran à apparaître est l'écran *Setup Summary*. L'utilitaire Web contient douze onglets principaux : Setup, Port Management, VLAN Management, Statistics, ACL, Security, QoS (Quality of Service), Spanning Tree, Multicast, SNMP, Admin et Logout. Le fait de cliquer sur l'un des onglets principaux permet d'afficher d'autres onglets.



REMARQUE : les DEL affichées dans l'utilitaire Web ne sont pas les mêmes que celles situées sur le panneau avant du commutateur. Les DEL du panneau avant affichent différentes informations d'état, décrites dans le *Chapitre 2 : Présentation du commutateur*.

Les DEL de l'écran Setup Summary fournissent des informations d'état sur les ports correspondants. La DEL verte indique qu'une connexion a été établie ; inversement, la DEL grise signale l'absence de connexion. La DEL orange signale que le port a été fermé par l'administrateur. Lorsque vous cliquez sur la DEL d'un port, les statistiques relatives à ce port s'affichent.



REMARQUE : une fois la configuration effectuée à l'aide de l'utilitaire Web, vous devrez peut-être actualiser la page pour que la mise à jour de la configuration soit prise en compte.



Figure 5-1 : Écran Login

Onglet Setup - Summary

L'écran *Summary* fournit des informations (périphérique et système) sur le commutateur.

Device Information

System Name. Affiche le nom du commutateur, si vous avez entré un nom dans l'onglet Setup - Network Settings.

IP Address. L'adresse IP du commutateur s'affiche ici (vous pouvez la configurer dans l'onglet Setup - Network Settings).

Subnet Mask. Le masque de sous-réseau du commutateur s'affiche ici (vous pouvez le configurer dans l'onglet Setup - Network Settings).

DNS Servers. Les serveurs DNS s'affichent ici (vous pouvez les configurer dans l'onglet Setup - Network Settings).

Default Gateway. La passerelle par défaut s'affiche ici (vous pouvez la configurer dans l'onglet Setup - Network Settings).

Address Mode. Indique si le commutateur est configuré à l'aide d'une adresse IP statique ou dynamique (vous pouvez la configurer dans l'onglet Setup - Network Settings).

Base MAC Address. Il s'agit de l'adresse MAC du commutateur.

System Information

Serial Number. Le numéro de série du produit est affiché à cet emplacement.

Model Name. Il s'agit du numéro de modèle et du nom du commutateur.

Hardware Version. Le numéro de version des composants matériels du commutateur s'affiche ici.

Boot Version. Indique la version de l'amorçage système en cours d'utilisation sur le périphérique.

Firmware Version. Le numéro de version du micrologiciel s'affiche ici.

System Location. L'emplacement du système s'affiche ici (vous pouvez le configurer dans l'onglet Setup - Network Settings).

System Contact. L'information de contact de ce commutateur s'affiche ici (vous pouvez la configurer dans l'onglet Setup - Network Settings).

System Up Time. Affiche la durée écoulée depuis la dernière réinitialisation du commutateur.

Current Time. L'heure système s'affiche ici (vous pouvez la configurer dans l'onglet Setup - Time).

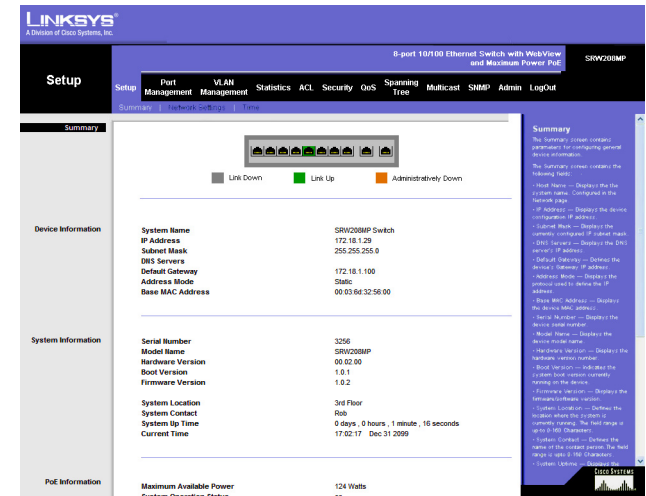


Figure 5-2 : Setup - Summary

PoE Information



REMARQUE : la section d'écran *PoE Information* apparaît uniquement dans l'écran Summary des modèles SRW208P et SRW208MP.

Maximum Available Power. Indique l'alimentation maximale que peut fournir le périphérique.

System Operation Status. Indique si la fonction PoE (Power over Ethernet) est activée ou désactivée.

Main Power Consumption. Affiche l'alimentation actuellement utilisée.

Onglet Setup - Network Settings

L'écran *Network Settings* permet d'affecter des paramètres DHCP ou IP statiques à des interfaces, ainsi que des passerelles par défaut.

Identification

System Name. Ce champ permet d'affecter un nom de système.

System Location. Ce champ est utilisé pour la saisie d'une description de l'emplacement du commutateur (3ème étage, par exemple).

System Contact. Saisissez le nom du contact administratif dans ce champ.

System Object ID. L'identificateur d'objet système s'affiche ici.

Base MAC Address. Il s'agit de l'adresse MAC du commutateur.

IP Configuration

Management VLAN. Cette liste déroulante permet de sélectionner le VLAN de gestion.

IP Address Mode. Cette liste déroulante permet de sélectionner la configuration d'adresse IP statique ou dynamique.

Host Name. Entrez ici le nom d'hôte DHCP.

IP Address. Si vous utilisez une adresse IP statique, entrez-la dans ce champ.

Subnet Mask. Entrez le masque de sous-réseau de l'adresse IP actuellement configurée.

Default Gateway. Entrez l'adresse IP de la passerelle par défaut.

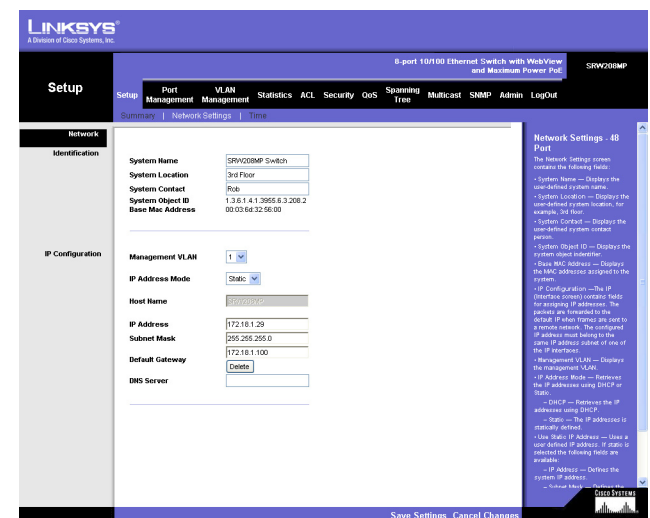


Figure 5-3 : Setup - Network Settings

DNS Server. Entrez les informations sur le serveur DNS principal.

Cliquez sur le bouton **Save Settings** pour enregistrer vos modifications ou sur le bouton **Cancel Changes** pour les annuler.

Onglet Setup - Time

L'écran *Time* permet de configurer les paramètres d'heure applicables au commutateur.

Set Time

Use System Time. Lorsque cette option est sélectionnée, l'horloge locale est utilisée.

Use SNTP Time. Si cette option est sélectionnée, l'heure est synchronisée sur un serveur SNTP (Simple Network Time Protocol).

Local Time

Hours. Vous pouvez entrer l'heure dans ce champ.

Minutes. Vous pouvez entrer les minutes dans ce champ.

Seconds. Vous pouvez entrer les secondes dans ce champ.

Month. Vous pouvez entrer le mois dans ce champ.

Day. Vous pouvez entrer le jour dans ce champ.

Year. Vous pouvez entrer l'année dans ce champ.

Time Zone. Entrez l'écart entre l'heure GMT (Greenwich Mean Time) et l'heure locale.

Daylight Saving

Daylight Saving. Sélectionnez **Daylight Saving** pour activer cette option au niveau du commutateur. Si le commutateur doit utiliser l'heure d'été en vigueur aux États-Unis, sélectionnez **USA**. Si le commutateur doit utiliser l'heure d'été en vigueur en Europe, sélectionnez la valeur **European**. Si une autre heure d'été doit être utilisée, sélectionnez **Custom** et renseignez les champs *From* et *To*.

Time Set Offset (1-1440). Pour tous les pays autres que les États-Unis ou les pays européens, indiquez la durée de l'heure d'été. La valeur par défaut est **60** minutes.



Figure 5-4 : Setup - Time

From. Si vous avez sélectionné la valeur Other pour *Daylight Saving*, entrez la date et l'heure de début de l'heure d'été.

To. Si vous avez sélectionné la valeur *Other* pour le paramètre *Daylight Saving*, entrez la date et l'heure de fin de l'heure d'été.

Recurring. Si vous avez sélectionné la valeur *Other* pour *Daylight Saving* et que l'heure d'été a la même date de début et la même date de fin chaque année, sélectionnez **Recurring**.

From. Si vous avez sélectionné Recurring, entrez la date et l'heure de début de l'heure d'été.

To. Si vous avez sélectionné Recurring, entrez la date et l'heure de fin de l'heure d'été.

SNTP Servers

Server1. Entrez dans ce champ le nom du serveur SNTP principal.

Server2. Entrez dans ce champ le nom d'un serveur SNTP secondaire.

SNTP Polling Interval (60-86400). La valeur définie ici détermine la durée (en secondes) écoulée avant l'interrogation du serveur SNTP par le commutateur. La valeur par défaut est toutes les 1 024 secondes (17 minutes environ).

Cliquez sur le bouton **Save Settings** pour enregistrer vos modifications ou sur le bouton **Cancel Changes** pour les annuler.

Onglet Port Management - Port Settings

L'écran *Port Management - Port Settings* contient les paramètres de chaque port du commutateur.

Port. Numéro du port. Pour pouvoir utiliser un module SFP, cliquez sur le bouton **Détail** du port approprié (G1, G2).

Description. Affiche une brève description du port (pour la saisir, cliquez sur le bouton **Détail**).

Administrative Status. Vous pouvez déconnecter le port via la sélection de l'option Down. Lorsque l'option Up est sélectionnée, l'accès au port s'effectue normalement.

Link Status. Up indique qu'une connexion active a été établie sur un port ; Down signale l'absence de connexion active ou la déconnexion du port par l'administrateur.

Speed. La vitesse de connexion du port s'affiche ici. La vitesse ne peut être configurée que lorsque la fonction d'auto-négociation est désactivée sur ce port.

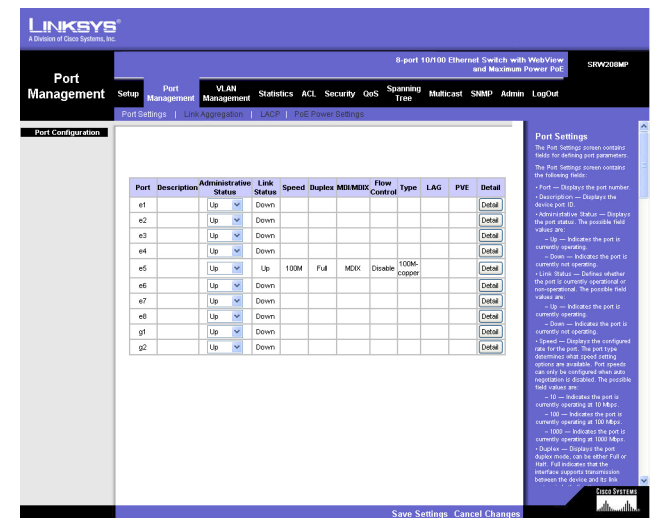


Figure 5-5 : Port Management - Port Settings

Duplex. Il s'agit du mode duplex, Full (la transmission s'effectue simultanément dans les deux sens) ou Half (la transmission s'effectue dans un sens à la fois uniquement). Vous ne pouvez configurer ce mode que lorsque la fonction d'auto-négociation est désactivée et que la vitesse du port est 10 Mbits/s ou 100 Mbits/s. Il ne peut pas être configuré sur les groupes LAG (Link Aggregation Groups).

MDI/MIDX. Il s'agit du statut MDI/MIDX du port. La valeur **MDI** est utilisée si le port est connecté à une station finale. La valeur **MDIX** est utilisée si le port est connecté à un concentrateur ou à un autre commutateur.

Flow Control. Il s'agit du statut de contrôle de flux du port. Il est actif lorsque le port utilise le mode Full Duplex.

LAG. Indique si le port fait partie d'un LAG.

Type. Affiche le type de port.

PVE. Si un port est de type PVE (Private VLAN Edge), il ignore la base de données de transfert et achemine toute diffusion individuelle et multidiffusion vers une liaison montante. Les liaisons montantes peuvent être des ports ou des LAG.

Detail. Le bouton Detail permet d'ouvrir l'écran Port Configuration Detail.

Écran Port Configuration Detail

Port. Numéro du port.

Description. Affiche une brève description du port (pour la saisir, cliquez sur le bouton **Detail**).

Port Type. Type du port.

Admin Status. Vous pouvez déconnecter le port via la sélection de l'option Down. Lorsque l'option Up est sélectionnée, l'accès au port s'effectue normalement.

Current Port Status. L'état actuel du port s'affiche ici.

Reactivate Suspended Port. Si vous souhaitez réactiver un port qui a été interrompu, cliquez sur la case à cocher.

Operational Status. Indique si le port est actif.

Admin Speed. La vitesse du port peut être modifiée dans ce champ.

Current Port Speed. La vitesse actuelle du port s'affiche dans ce champ.

Admin Duplex. Le mode duplex peut être modifié dans ce champ.

Current Duplex Mode. Il s'agit du mode duplex du port.



REMARQUE : PVE ne s'applique pas au SRW208.

Figure 5-6 : Port Settings - Port Configuration Detail

Auto Negotiation. Vous pouvez activer ou désactiver la fonction d'auto-négociation du port. Si vous utilisez un module SFP, la fonction Auto Negotiation du port correspondant doit être définie sur Disable.

Current Auto Negotiation. Paramétrage actuel de la fonction Auto Negotiation du port.

Admin Advertisement. Indique les capacités à signaler par le port. Vous pouvez sélectionner plusieurs options, ou encore sélectionner Max Capability pour couvrir la totalité des options. Les options disponibles sont les suivantes :

- **Max Capability.** Indique que les vitesses de port et les valeurs de mode duplex peuvent être acceptées.
- **10 Half.** Indique que le port est en mode semi-duplex 10 Mbits/s.
- **10 Full.** Indique que le port est en mode Full Duplex 10 Mbits/s.
- **100 Half.** Indique que le port est en mode semi-duplex 100 Mbits/s.
- **100 Full.** Indique que le port est en mode Full Duplex 100 Mbits/s.
- **1000.** Indique que le port est en mode Full Duplex 1 000 Mbits/s.

Current Advertisement. Le port signale ses capacités au port voisin afin de commencer le processus de négociation. Ce champ affiche le paramétrage signalé par le port.

Neighbor Advertisement. Le port voisin (port auquel l'interface sélectionnée est connectée) signale ses capacités au port, afin de commencer le processus de négociation. Ce champ affiche le paramétrage actuel du port voisin.

Back Pressure. Vous pouvez activer ou désactiver la fonction Back Pressure du port sélectionné.

Current Back Pressure. Indique si la fonction Back Pressure est activée ou désactivée sur le port actuellement sélectionné.

Flow Control. Vous pouvez activer ou désactiver la fonction de contrôle de flux Flow Control du port sélectionné.

Current Flow Control. Indique si la fonction Flow Control est activée ou désactivée sur le port actuellement sélectionné.

MDI/MDIX. Sélectionnez la valeur **Auto** si vous souhaitez que le port détecte automatiquement le type de câble. Sélectionnez **MDI** si le port est connecté à une station finale. Sélectionnez **MDIX** si le port est connecté à un concentrateur ou à un autre commutateur.

Current MDI/MDIX. Il s'agit du statut MDI/MDIX actuel du port.

PVE. Si un port est de type PVE (Private VLAN Edge), il ignore la base de données de transfert et achemine toute diffusion individuelle et multidiffusion vers une liaison montante.



REMARQUE : tous les ports du même groupe PVE doivent rejoindre le même groupe VLAN.

Cliquez sur le bouton **Save Settings** pour enregistrer ces modifications.

Onglet Port Management - Link Aggregation

LAG. Indique si le port fait partie d'un LAG.

Description. Description de ce LAG.

Admin Status. Statut d'administration du LAG. La valeur Up indique que le LAG est disponible. La valeur Down indique que l'administrateur a déconnecté le port. Lorsque vous modifiez cette option, veuillez à cliquer ensuite sur le bouton **Save Settings**.

Type. Le type de LAG s'affiche ici.

Link Status. Le statut de la liaison s'affiche ici.

Speed. La vitesse de connexion s'affiche ici.

Duplex. Le mode duplex s'affiche ici pour la connexion.

Flow Control. Affiche le statut du contrôle de flux du LAG. Il est actif lorsque le port utilise le mode Full Duplex.

LAG Mode. Affiche le statut du LAG (On, Off ou Not Present).

Bouton Detail. Le bouton Detail permet d'afficher l'écran Link Aggregation Detail.

Écran Link Aggregation Detail

LAG Configuration

LAG. Nombre de LAG sélectionnés.

Description. Vous pouvez inclure ici une description générale à titre de référence.

LACP. Indique si le LAG est en mode LACP (Link Aggregation Control Protocol).

LAG Type. Types de port incluant le LAG.

Administrative Status. Active ou désactive le transfert du trafic via le LAG sélectionné.

Current Status. Indique si le LAG est en cours de fonctionnement.

Reactivate Suspended LAG. Réactive le LAG si ce dernier a été désactivé suite à un verrouillage de port ou à une opération ACL.

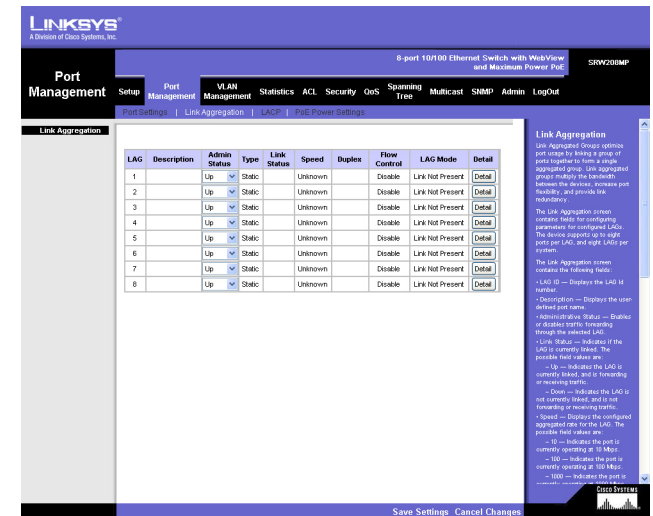


Figure 5-7 : Port Management - Link Aggregation

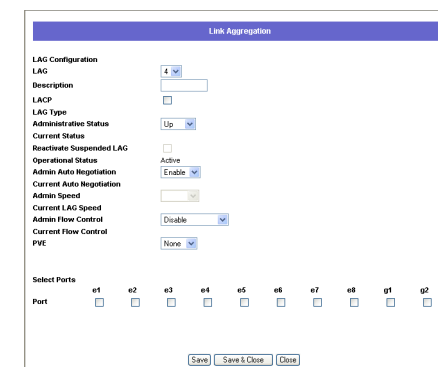


Figure 5-8 : Link Aggregation - Link Aggregation Detail

Admin Auto Negotiation. Active ou désactive la fonction de négociation automatique sur le LAG. Auto Speed est un protocole utilisé entre deux partenaires de liaison permettant à un LAG d'indiquer à son partenaire sa vitesse de transmission, son mode duplex et ses capacités de contrôle de flux (la valeur par défaut de contrôle de flux est désactivée).

Current Auto Negotiation. Paramétrage actuel de l'option de négociation automatique.

Admin Speed. Vitesse configurée de fonctionnement du LAG.

Current LAG Speed. Vitesse actuelle de fonctionnement du LAG.

Admin Flow Control. Active ou désactive le contrôle de flux, ou active la fonction de négociation automatique du contrôle de flux sur le LAG.

Current Flow Control. Valeur de contrôle de flux affectée par l'utilisateur.

PVE. Affiche le groupe PVE dans lequel le LAG est configuré.

Select Ports

Ports. Affiche les ports membres du LAG sélectionné.

Onglet Port Management - LACP

Les ports agrégés peuvent être liés au sein de groupes de ports. Chaque groupe se compose de ports dont la vitesse et le mode de fonctionnement (Full Duplex) sont identiques.

Vous pouvez configurer manuellement les liaisons agrégées, ou encore les définir automatiquement via l'activation du protocole LACP (Aggregation Control Protocol) sur les liaisons appropriées. Les ports agrégés peuvent être liés au sein de groupes de ports. Chaque groupe se compose de ports dont la vitesse est identique. L'écran LACP contient des champs permettant de configurer les LAG LACP.

LACP System Priority (1-65535). Indique la valeur de priorité LACP globale. La plage acceptée est comprise entre 1 et 65535. La valeur par défaut est 1.

Port. Définit le numéro de port auquel sont affectées les valeurs de dépassement de délai et de priorité.

LACP Port Priority. Définit la valeur de priorité LACP applicable au port. La plage de valeurs de ce champ est de 1 à 65535.

LACP Timeout. Dépassement de délai LACP administratif. Vous pouvez sélectionner une valeur courte ou longue de dépassement de délai. La valeur longue correspond à la valeur par défaut.

Admin Key. Un canal ne peut se former qu'entre ports possédant la même clé d'administration. Cela s'applique uniquement aux ports situés sur le même commutateur.

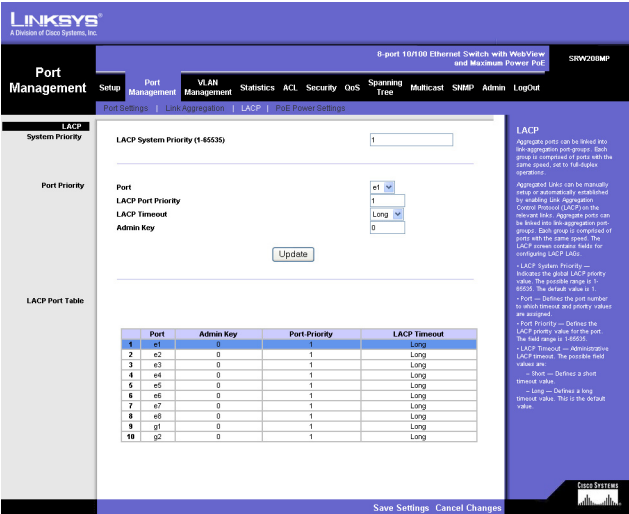


Figure 5-9 : Port Management - LACP

Onglet Port Management - PoE Power Settings



REMARQUE : la page Modify PoE affiche les ports PoE actuellement configurés. Cette option ne s'affiche que pour les modèles SRW208P et SRW208MP.

Port. Affiche le numéro du port sélectionné.

Admin Status. Indique si PoE est activé ou désactivé sur le port.

Priority. Indique la valeur de priorité PoE du port. Les valeurs de champ possibles sont les suivantes : Critical, High et Low. La valeur par défaut est Low.

Power Allocation (milliwatts). Indique le niveau réel de puissance que le périphérique peut fournir.

Mode. Indique si le port est activé en vue de l'utilisation de PoE.

Power Consumption (milliwatts). Indique le niveau de puissance utilisé par le périphérique.

Onglet VLAN Management - Create VLAN

L'écran Create VLAN contient des informations et des paramètres globaux destinés à la configuration et à l'utilisation des VLAN.

Single VLAN

ID de VLAN (2-4094). Indique l'ID du VLAN configuré. Vous pouvez créer jusqu'à 256 VLAN. Ce champ est utilisé pour ajouter individuellement des VLAN. Pour ajouter l'ID de VLAN défini, cliquez sur le bouton **Add**.

VLAN Name. Affiche le nom de VLAN défini par l'utilisateur.

VLAN Range

VLAN Range. Indique la plage de réseaux VLAN en cours de configuration. Pour ajouter la plage d'ID de réseaux VLAN définie, appuyez sur le bouton **Add Range**.

VLAN Table

Le tableau de réseaux VLAN répertorie tous les réseaux VLAN configurés. Il affiche l'ID, le nom et le statut des réseaux VLAN. Pour supprimer un VLAN, cliquez sur le bouton **Remove**.

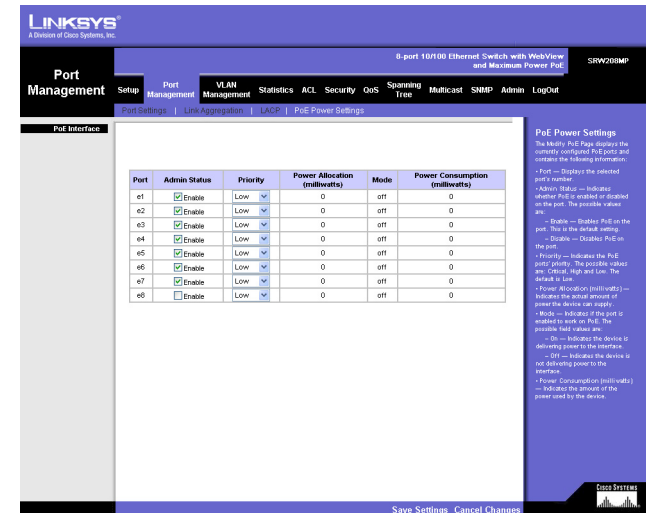


Figure 5-10 : Port Management - PoE Power Settings



Figure 5-11 : VLAN Management - Create VLAN



REMARQUE : les VLAN créés dynamiquement à l'aide de GVRP portent un nom VLAN indéfini (« Undefined »).

Onglet VLAN Management - Port Settings

L'écran VLAN Port Settings contient les paramètres permettant de gérer les ports inclus dans un réseau VLAN. L'ID de VLAN de port par défaut (PVID) est configuré dans l'écran VLAN Port Settings. Tous les paquets non balisés parvenant au périphérique sont balisés par le PVID des ports.

Port. Numéro de port inclus dans le VLAN.

Mode. Indique le mode applicable au port. Les valeurs possibles sont les suivantes :

- **General.** Le port appartient aux réseaux VLAN, et chacun d'entre eux est défini par l'utilisateur comme étant balisé ou non balisé (mode Full 802.1Q).
- **Access.** Le port appartient à un seul réseau VLAN non balisé. Lorsqu'un port est en mode Access, les types de paquets acceptés sur le port (type de paquet) ne peuvent pas être spécifiés. Vous ne pouvez pas non plus activer/désactiver le filtrage entrant sur les ports en mode Access.
- **Trunk.** Le port appartient aux réseaux VLAN dans lesquels tous les ports sont balisés (à l'exception d'un seul réseau VLAN natif).

Acceptable Frame Type. Type de paquet accepté sur le port. Les valeurs possibles sont les suivantes :

- **Admit Tag Only.** Indique que seuls les paquets balisés sont acceptés sur le port.
- **Admit All.** Indique que les paquets balisés et non balisés sont acceptés sur le port.

PVID. Permet d'affecter un ID de VLAN aux paquets non balisés. Les valeurs possibles sont comprises entre 2 et 4094. Le réseau VLAN 4095 est défini de façon standard comme étant le VLAN éliminé. Les paquets classés dans le VLAN éliminé sont supprimés.

Ingress Filtering. Active ou désactive la fonction de filtrage entrant sur le port. Le filtrage entrant permet d'éliminer les paquets qui n'incluent pas de port entrant.

LAG. Indique le LAG auprès duquel le réseau VLAN est défini.

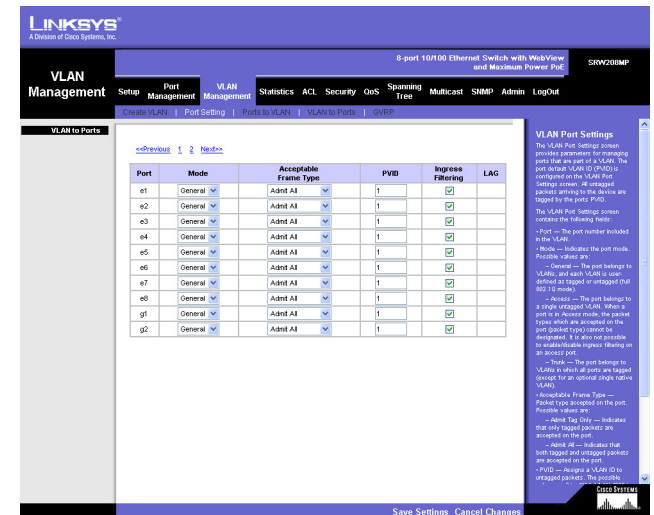


Figure 5-12 : VLAN Management - Port Settings

Onglet VLAN Management - Ports to VLAN

L'écran Ports to VLAN contient des champs permettant de configurer des ports pour un réseau VLAN. L'ID de VLAN de port par défaut (PVID) est configuré dans l'écran Create VLAN. Tous les paquets non balisés parvenant au périphérique sont balisés par le PVID des ports.

L'écran Ports to VLAN contient un tableau de ports indiquant les paramètres VLAN applicables à chaque port. Pour que les ports deviennent membres du réseau VLAN, vous devez sélectionner et configurer les options de configuration présentées.

VLAN. Numéro du réseau VLAN.

Access. Indique que le port appartient à un seul réseau VLAN non balisé. Lorsqu'un port est en mode Access, les types de paquets acceptés sur le port ne peuvent pas être spécifiés. Le filtrage entrant ne peut pas être activé/désactivé sur un port d'accès.

Trunk. Indique que le port appartient à des réseaux VLAN dans lesquels tous les ports sont balisés, à l'exception d'un port qui peut être non balisé.

General. Indique que le port appartient à des réseaux VLAN, et que chacun d'entre eux est défini par l'utilisateur comme étant balisé ou non balisé (mode Full 802.1Q).

Tagged. Définit l'interface comme étant un membre balisé de réseau VLAN. Tous les paquets transmis par l'interface sont balisés. Les paquets contiennent des informations sur les réseaux VLAN.

Untagged. Les paquets transmis par l'interface sont non balisés.

Forbidden. Les ports interdits ne sont pas inclus dans le réseau VLAN.

Exclue. Exclut l'interface du réseau VLAN. Toutefois, l'interface peut être ajoutée au réseau VLAN via le protocole GVRP.

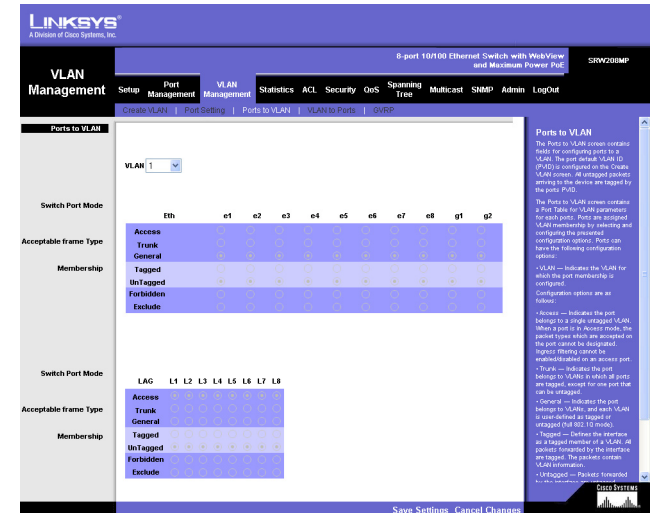


Figure 5-13 : VLAN Management - Ports to VLAN

Onglet VLAN Management - VLAN to Ports

L'écran VLAN to Ports contient des champs permettant de configurer des réseaux VLAN pour un port.

Interface. Affiche le numéro d'interface.

Mode. Indique le mode de configuration port/VLAN. Les valeurs de champ possibles sont les suivantes :

- **General.** Indique que le port appartient à des réseaux VLAN, et que chacun d'entre eux est défini par l'utilisateur comme étant balisé ou non balisé (mode Full 802.1Q).
- **Access.** Indique que le port appartient à un seul réseau VLAN non balisé. Lorsqu'un port est en mode Access, les types de paquets acceptés sur le port ne peuvent pas être spécifiés. Le filtrage entrant ne peut pas être activé/désactivé sur un port d'accès.
- **Trunk.** Indique que le port appartient à des réseaux VLAN dans lesquels tous les ports sont balisés, à l'exception d'un port qui peut être non balisé.

Join VLAN. Définit les réseaux VLAN auxquels l'interface est jointe.

VLANs. Affiche la balise PVID.

LAG. Indique si le port est membre d'un LAG. S'il est membre d'un LAG, il ne peut pas être configuré auprès d'un VLAN. Le LAG auquel il appartient peut être configuré auprès d'un VLAN.

Écran Join VLAN Detail

L'écran Join VLAN Detail vous permet de sélectionner le réseau VLAN pour le port sélectionné et de déterminer s'il est balisé ou non. Il sera affiché avec un T s'il est balisé et avec U s'il n'est pas balisé.



Figure 5-14 : VLAN Management - VLAN to Ports

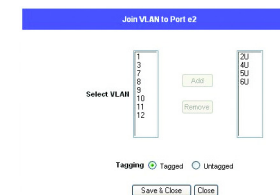


Figure 5-15 : VLAN to Ports - Join VLAN

Onglet VLAN Management - GVRP

Le protocole GVRP (GARP VLAN Registration Protocol) permet d'effectuer la distribution automatique d'informations de membres VLAN entre des ponts informés VLAN (VLAN-aware). Le protocole GVRP permet à des ponts informés VLAN de détecter automatiquement les mappages de ports entre réseaux VLAN et ponts, sans qu'il soit nécessaire de configurer individuellement chaque pont et d'enregistrer les membres de réseaux VLAN.

Les informations s'affichent dans les mêmes champs que les ports, mais représentent des informations LAG GVRP.

L'écran GVRP se divise en deux zones (GVRP et GVRP Table). Les définitions de champ de ces deux zones sont identiques.

Enable GVRP. Active et désactive GVRP sur le périphérique.

Interface. Affiche l'interface sur laquelle le protocole GVRP est activé. Les valeurs de champ possibles sont les suivantes :

- **Port.** Indique le numéro de port sur lequel le protocole GVRP est activé.
- **LAG.** Indique le numéro de LAG sur lequel le protocole GVRP est activé.

GVRP State. Si cette case est cochée, le protocole GVRP est activé sur l'interface.

Dynamic VLAN Creation. Si cette case est cochée, la création de VLAN dynamique est activée sur l'interface.

GVRP Registration. Si cette case est cochée, l'enregistrement de réseau VLAN via le protocole GVRP est activé sur le périphérique.

Le bouton **Update** permet d'ajouter le paramètre GVRP configuré au tableau situé au bas de l'écran.

Onglet Statistics - RMON Statistics

L'écran RMON Statistics contient des champs qui permettent d'afficher des informations sur l'utilisation du périphérique et sur les erreurs survenues sur ce dernier.

Interface. Indique le périphérique pour lequel les statistiques sont affichées. Les valeurs de champ possibles sont les suivantes :

- **Port.** Définit le port spécifique pour lequel les statistiques RMON sont affichées.
- **LAG.** Définit le LAG spécifique pour lequel les statistiques RMON sont affichées.

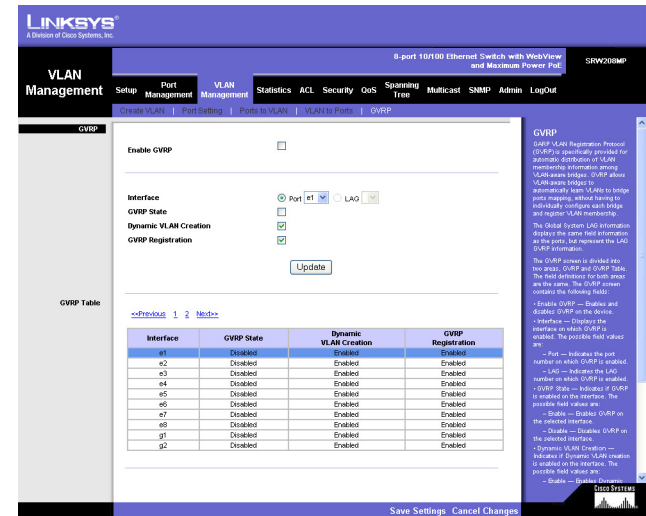


Figure 5-16 : VLAN Management - GVRP

Refresh Rate. Définit la durée écoulée avant l'actualisation des statistiques sur l'interface. Les valeurs de champ possibles sont les suivantes :

- **No Refresh.** Indique que les statistiques RMON ne sont pas actualisées.
- **15 Sec.** Indique que les statistiques RMON sont actualisées toutes les 15 secondes.
- **30 Sec.** Indique que les statistiques RMON sont actualisées toutes les 30 secondes.
- **60 Sec.** Indique que les statistiques RMON sont actualisées toutes les 60 secondes.

Drop Events. Affiche le nombre d'événements supprimés sur l'interface depuis la dernière actualisation du périphérique.

Received Bytes (Octets). Affiche le nombre d'octets reçus sur l'interface depuis la dernière actualisation du périphérique. Ce nombre inclut les paquets erronés et les octets FCS, mais exclut les bits de trame.

Received Packets. Affiche le nombre de paquets reçus sur l'interface, y compris les paquets erronés, les paquets de multidiffusion et de diffusion, depuis la dernière actualisation du périphérique.

Broadcast Packets Received. Affiche le nombre de packets de diffusion corrects reçus sur l'interface depuis la dernière actualisation du périphérique. Ce nombre n'inclut pas les paquets de multidiffusion.

Multicast Packets Received. Affiche le nombre de packets de multidiffusion corrects reçus sur l'interface depuis la dernière actualisation du périphérique.

CRC & Align Errors. Affiche le nombre d'erreurs CRC et d'alignement survenues sur l'interface depuis la dernière actualisation du périphérique.

Undersize Packets. Affiche le nombre de paquets de taille trop faible (inférieure à 64 octets) reçus sur l'interface depuis la dernière actualisation du périphérique.

Oversize Packets. Affiche le nombre de paquets de taille trop élevée (supérieure à 1 518 octets) reçus sur l'interface depuis la dernière actualisation du périphérique.

Fragments. Affiche le nombre de fragments (paquets de moins de 64 octets, en excluant les bits de trame mais en incluant les octets FCS) reçus sur l'interface depuis la dernière actualisation du périphérique.

Jabbers. Affiche le nombre total de paquets reçus dont la longueur dépasse 1 518 octets. Ce chiffre exclut les bits de trame, mais inclut les octets FCS affichant soit une mauvaise séquence FCS (Frame Check Sequence) avec un nombre intégral d'octets (erreur FCS), soit une mauvaise séquence FCS avec un nombre non intégral d'octets (erreur d'alignement). La plage de détection correspondante est comprise entre 20 ms et 150 ms.

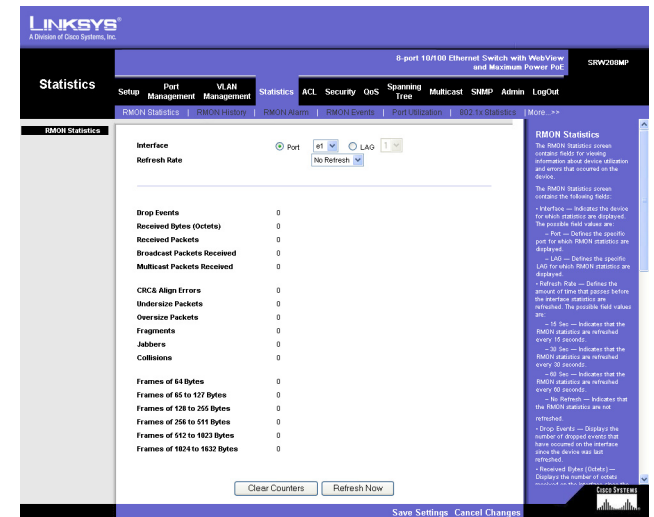


Figure 5-17 : Statistics - RMON Statistics

Collisions. Affiche le nombre de collisions reçues sur l'interface depuis la dernière actualisation du périphérique.

Frames of xx Bytes. Nombre de trames de xx octets reçues sur l'interface depuis la dernière actualisation du périphérique.

Bouton **Clear Counters.** Cette option permet de réinitialiser tous les compteurs statistiques.

Bouton **Refresh Now.** Utilisez cette option pour actualiser les statistiques.

Onglet Statistics - RMON History

L'écran RMON History contient des informations sur des échantillons de données en provenance des ports. Par exemple, ces échantillons peuvent inclure des définitions d'interface ou des périodes d'interrogation.

L'écran RMON History Control se divise en deux zones (RMON History et Log Table).

Source Interface. Affiche l'interface dont proviennent les exemples d'historique. Les valeurs de champ possibles sont les suivantes :

- **Port.** Indique le port dont proviennent les informations RMON.
- **LAG.** Indique le port dont proviennent les informations RMON.

Sampling Interval. Indique la durée (en secondes) d'extraction des échantillons sur les ports. La plage valide est comprise entre 1 et 3600. La valeur par défaut est 1 800 secondes (soit 30 minutes).

Max No. of Samples to Keep. Indique le nombre d'échantillons à enregistrer.

Owner. Affiche la station ou l'utilisateur RMON ayant demandé les informations RMON. La plage valide est comprise entre 0 et 20 caractères.

Le bouton **Add to List** permet d'ajouter l'échantillon RMON configuré au tableau de journaux, situé au bas de l'écran.

Log Table

Sampling Requested. Affiche le nombre d'échantillons à enregistrer. La plage valide est comprise entre 1 et 65535. La valeur par défaut est 50.

Current Number of Samples. Affiche le nombre actuel d'échantillons extraits.

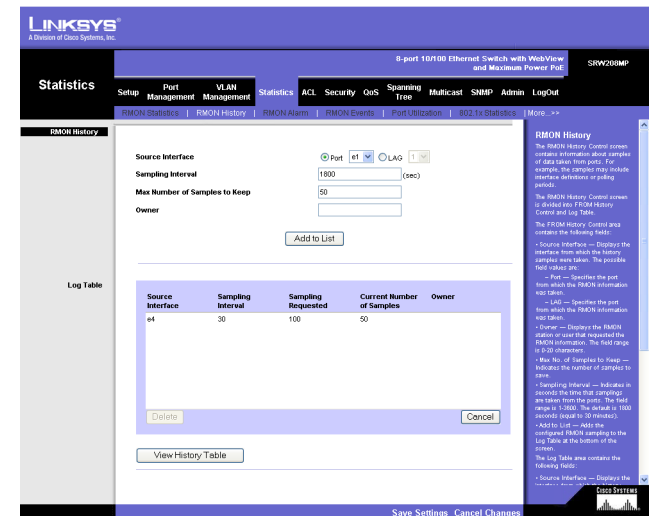


Figure 5-18 : Statistics - RMON History

RMON History

L'écran RMON History contient des échantillons de statistiques réseau propres aux différentes interfaces. Chaque entrée de tableau représente toutes les valeurs de compteurs compilées au cours d'un échantillonnage.

History Entry No. Affiche le numéro d'entrée figurant dans le tableau d'historique.

Owner. Affiche la station ou l'utilisateur RMON ayant demandé les informations RMON. La plage valide est comprise entre 0 et 20 caractères.

Sample No. Indique le numéro d'échantillon à partir duquel les statistiques ont été prélevées.

Drop Events. Affiche le nombre d'événements supprimés sur l'interface depuis la dernière actualisation du périphérique.

Received Bytes (Octets). Affiche le nombre d'octets reçus sur l'interface depuis la dernière actualisation du périphérique. Ce nombre inclut les paquets erronés et les octets FCS, mais exclut les bits de trame.

Received Packets. Affiche le nombre de paquets reçus sur l'interface depuis la dernière actualisation du périphérique, y compris les paquets erronés, les paquets de multidiffusion et de diffusion.

Broadcast Packets. Affiche le nombre de paquets de diffusion corrects reçus sur l'interface depuis la dernière actualisation du périphérique. Ce nombre n'inclut pas les paquets de multidiffusion.

Multicast Packets. Affiche le nombre de paquets de multidiffusion corrects reçus sur l'interface depuis la dernière actualisation du périphérique.

CRC Align Errors. Affiche le nombre d'erreurs CRC et d'alignement survenues sur l'interface depuis la dernière actualisation du périphérique.

Undersize Packets. Affiche le nombre de paquets de taille trop faible (inférieure à 64 octets) reçus sur l'interface depuis la dernière actualisation du périphérique.

Oversize Packets. Affiche le nombre de paquets de taille trop élevée (supérieure à 1 518 octets) reçus sur l'interface depuis la dernière actualisation du périphérique.

Fragments. Affiche le nombre de fragments (paquets de moins de 64 octets, en excluant les bits de trame mais en incluant les octets FCS) reçus sur l'interface depuis la dernière actualisation du périphérique.

Jabbers. Affiche le nombre total de paquets reçus dont la longueur dépasse 1 518 octets. Ce chiffre exclut les bits de trame, mais inclut les octets FCS affichant soit une mauvaise séquence FCS (Frame Check Sequence)

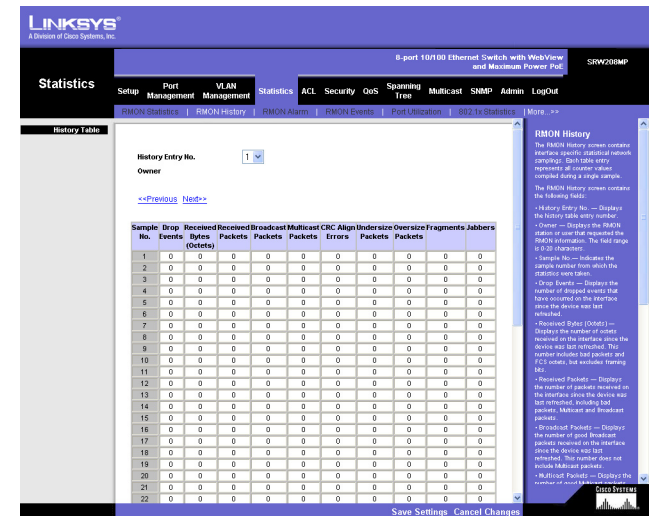


Figure 5-19 : Tableau RMON History

avec un nombre intégral d'octets (erreur FCS), soit une mauvaise séquence FCS avec un nombre non intégral d'octets (erreur d'alignement). La plage de détection correspondante est comprise entre 20 ms et 150 ms.

Collisions. Affiche le nombre de collisions reçues sur l'interface depuis la dernière actualisation du périphérique.

Utilization. Affiche le pourcentage d'interface utilisé.

Onglet Statistics - RMON Alarm

L'écran RMON Alarm contient des champs qui permettent de définir des alarmes réseau. Les alarmes réseau ont lieu lorsqu'un incident ou un événement réseau est détecté. La présence de seuils en augmentation ou en diminution génère des événements.

Alarm Entry. Indique une alarme spécifique.

Source Interface. Affiche l'interface pour laquelle les statistiques RMON sont affichées. Les valeurs de champ possibles sont les suivantes :

- **Port.** Affiche les statistiques RMON pour le port sélectionné.
- **LAG.** Affiche les statistiques RMON pour le LAG sélectionné.

Counter Name. Affiche la variable MIB sélectionnée.

Sample Type. Définit la méthode d'échantillonnage utilisée pour la variable sélectionnée et compare cette valeur avec les seuils. Les valeurs de champ possibles sont les suivantes :

- **Absolute.** Compare directement les valeurs avec les seuils en fin d'intervalle d'échantillonnage.
- **Delta.** Soustrait la dernière valeur échantillonnée de la valeur en cours. L'écart obtenu est comparé au seuil.

Rising Threshold. Affiche la valeur de compteur qui déclenche l'alarme de seuil en augmentation. Le seuil en augmentation est affiché en haut des histogrammes. Chaque variable surveillée porte une couleur différente.

Rising Event. Affiche la méthode de reporting des alarmes. Les valeurs de champ possibles sont les suivantes :

- **LOG.** Indique qu'il n'existe pas de méthode d'enregistrement applicable au périphérique ou au système de gestion. Si le périphérique n'est pas réinitialisé, l'entrée reste dans le tableau de journaux.
- **TRAP.** Indique qu'une interception SNMP est générée et envoyée via la méthode d'envoi d'interceptions. Cette interception peut également être enregistrée à l'aide de cette méthode.

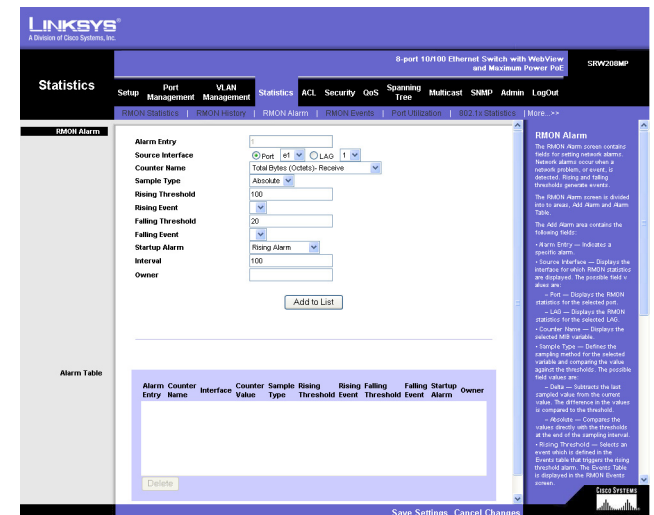


Figure 5-20 : Statistics - RMON Alarm

- **Both.** Indique que les deux méthodes (journal et interception) sont utilisées pour le reporting d'alarmes.

Falling Threshold. Affiche la valeur de compteur en diminution qui déclenche l'alarme de seuil en diminution. Le seuil en diminution est présenté sous forme graphique (dans la partie supérieure des histogrammes). Chaque variable surveillée porte une couleur différente.

Falling Event. Affiche la méthode de reporting des alarmes. Les valeurs de champ possibles sont les suivantes :

- **LOG.** Indique qu'il n'existe pas de méthode d'enregistrement applicable au périphérique ou au système de gestion. Si le périphérique n'est pas réinitialisé, l'entrée reste dans le tableau de journaux.
- **TRAP.** Indique qu'une interception SNMP est générée et envoyée via la méthode d'envoi d'interceptions. Cette interception peut également être enregistrée à l'aide de cette méthode.
- **Both.** Indique que les deux méthodes (journal et interception) sont utilisées pour le reporting d'alarmes.

Startup Alarm. Affiche le déclencheur qui active la création d'alarmes. L'augmentation est définie via le dépassement du seuil (valeur faible et valeur élevée).

Interval. Définit l'intervalle d'alarme, exprimée en secondes.

Owner. Affiche le périphérique ou l'utilisateur ayant défini l'alarme.

Le bouton **Add to List** permet d'ajouter l'entrée de tableau d'alarmes RMON.

La zone Alarm Table contient le champ supplémentaire suivant :

Counter Value. Affiche la valeur de compteur actuelle pour l'alarme spécifique.

Onglet Statistics - RMON Events

L'écran RMON Events contient des champs qui permettent de définir des événements RMON.

Add Event

Event Entry. Affiche l'événement.

Community. Affiche la communauté à laquelle appartient l'événement.

Description. Affiche la description de l'événement définie par l'utilisateur.

Type. Décrit le type d'événement. Les valeurs possibles sont les suivantes :

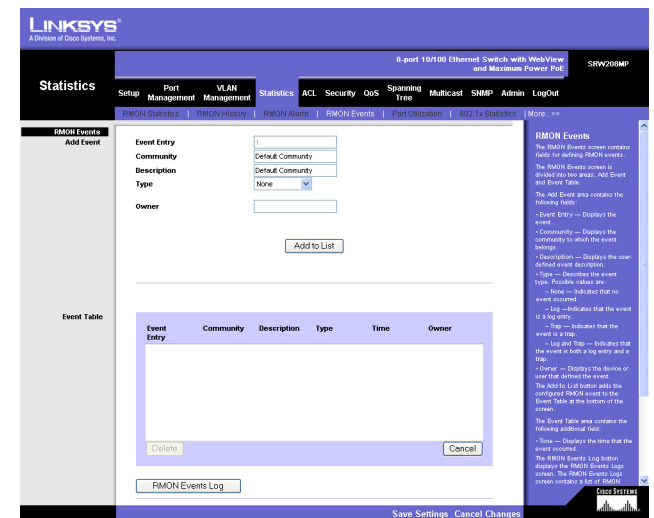


Figure 5-21 : Statistics - RMON Events

- **None.** Indique qu'aucun événement n'a eu lieu.
- **Log.** Indique que l'événement est une entrée de journal.
- **Trap.** Indique que l'événement est une interception.
- **Log and Trap.** Indique que l'événement est à la fois une entrée de journal et une interception.

Owner. Affiche le périphérique ou l'utilisateur ayant défini l'événement.

Le bouton **Add to List** permet d'ajouter l'événement RMON configuré au tableau des événements, situé au bas de l'écran.

La zone Event Table contient le champ supplémentaire suivant :

Time. Affiche l'heure à laquelle l'événement s'est produit.



Figure 5-22 : RMON Events - Events Log

Onglet Statistics - Port Utilization

L'écran Port Utilization affiche la quantité de ressources actuellement consommée par chaque interface. Les ports en vert fonctionnent normalement, tandis que les ports en rouge transfèrent actuellement une quantité de trafic réseau excessive.

Refresh Rate. Indique la durée écoulée avant l'actualisation des statistiques relatives à l'utilisation des ports. Les valeurs de champ possibles sont les suivantes :

- **No Refresh.** Indique que les statistiques ne sont pas actualisées.
- **15 Sec.** Indique que les statistiques sont actualisées toutes les 15 secondes.
- **30 Sec.** Indique que les statistiques sont actualisées toutes les 30 secondes.
- **60 Sec.** Indique que les statistiques sont actualisées toutes les 60 secondes.

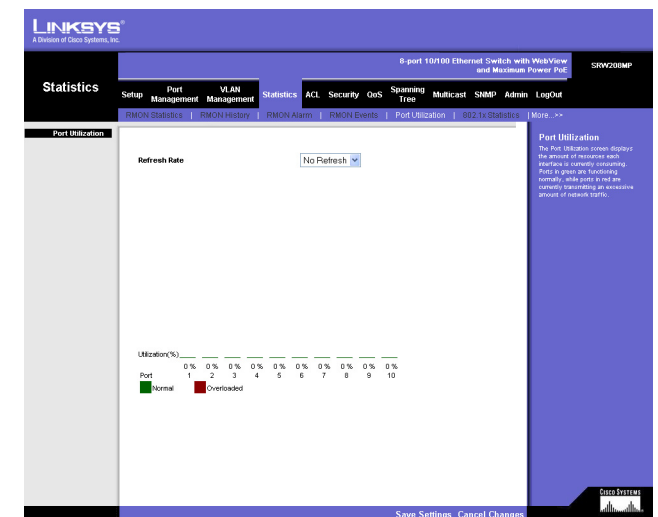


Figure 5-23 : Statistics - Port Utilization

Onglet Statistics - 802.1x Statistics

L'écran 802.1x Statistic contient des informations sur les paquets EAP reçus sur un port spécifique.

Port. Indique le port interrogé à des fins statistiques.

Refresh Rate. Définit la durée écoulée avant l'actualisation des statistiques EAP. Les valeurs de champ possibles sont les suivantes :

- **No Refresh.** Indique que les statistiques EAP ne sont pas actualisées.
- **15 Sec.** Indique que les statistiques EAP sont actualisées toutes les 15 secondes.
- **30 Sec.** Indique que les statistiques EAP sont actualisées toutes les 30 secondes.
- **60 Sec.** Indique que les statistiques EAP sont actualisées toutes les 60 secondes.

Name. Affiche la statistique 802.1x mesurée.

Description. Décrit la statistique 802.1x mesurée.

Packet. Affiche la quantité de paquets mesurée pour la statistique 802.1x.

Onglet Statistics - GVRP Statistics

L'écran GVRP Statistics contient les statistiques du périphérique pour GVRP.

L'écran GVRP se divise en deux zones (GVRP Statistics Table et GVRP Error Statistics Table). Les champs suivants sont identiques pour les deux tableaux :

Interface. Indique l'interface pour laquelle les statistiques sont affichées.

- **Port.** Indique que les statistiques de port sont affichées.
- **LAG.** Indique que les statistiques de LAG sont affichées.

Refresh Rate. Définit la durée écoulée avant l'actualisation des statistiques GVRP. Les valeurs de champ possibles sont les suivantes :

- **No Refresh.** Indique que les statistiques GVRP ne sont pas actualisées.
- **15 Sec.** Indique que les statistiques GVRP sont actualisées toutes les 15 secondes.

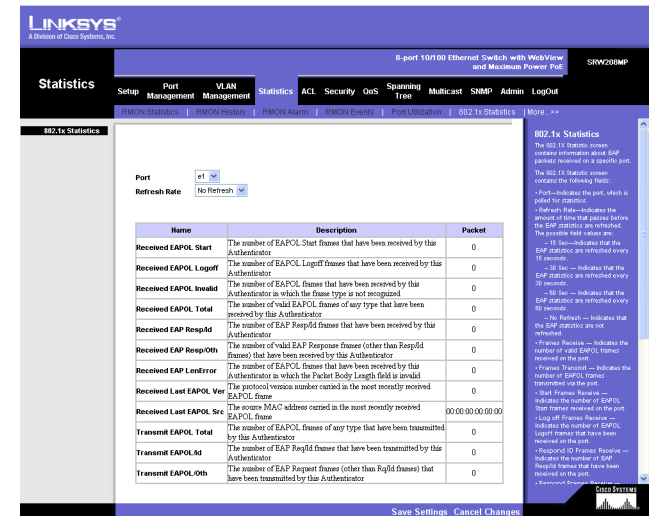


Figure 5-24 : Statistics - 802.1x Statistics

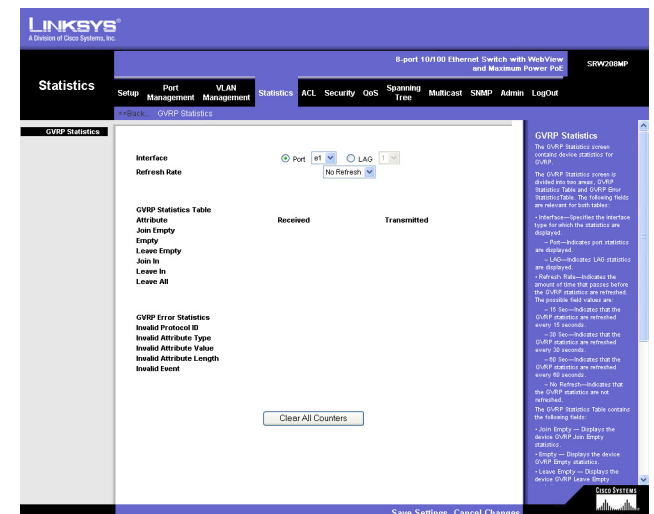


Figure 5-25 : Statistics - GVRP Statistics

- **30 Sec.** Indique que les statistiques GVRP sont actualisées toutes les 30 secondes.
- **60 Sec.** Indique que les statistiques GVRP sont actualisées toutes les 60 secondes.

Le tableau de statistiques GVRP contient les champs suivants :

Join Empty. Affiche les statistiques relatives à l'option GVRP Join Empty du périphérique.

Empty. Affiche les statistiques de l'option GVRP Empty du périphérique.

Leave Empty. Affiche les statistiques de l'option GVRP Leave Empty du périphérique.

Join In. Affiche les statistiques relatives à l'option GVRP Join In du périphérique.

Leave In. Affiche les statistiques de l'option GVRP Leave in du périphérique.

Leave All. Affiche les statistiques de l'option GVRP Leave all du périphérique.

Le tableau de statistiques d'erreurs GVRP contient les champs suivants :

Invalid Protocol ID. Affiche les statistiques sur l'erreur GVRP Invalid Protocol ID du périphérique.

Invalid Attribute Type. Affiche les statistiques sur l'erreur GVRP Invalid Attribute ID du périphérique.

Invalid Attribute Value. Affiche les statistiques sur l'erreur GVRP Invalid Attribute Value du périphérique.

Invalid Attribute Length. Affiche les statistiques sur l'erreur GVRP Invalid Attribute Length du périphérique.

Invalid Events. Affiche les statistiques sur l'erreur GVRP Invalid Events du périphérique.

Le bouton **Clear All Counters** permet de réinitialiser tous les tableaux.

Onglet ACL - IP Based ACL

La liste de contrôle d'accès (ACL) basée IP contient des informations sur la définition des ACL basées IP.

ACL Name. Affiche les ACL basées IP définies par l'utilisateur.

New ACL Name. Définit une nouvelle ACL basée IP définie par l'utilisateur.

Delete ACL. Supprime l'ACL sélectionnée.

Action. Indique l'action affectée au paquet correspondant à l'ACL. Les paquets sont soit transférés, soit supprimés. Par ailleurs, le port peut être arrêté, une interception peut être envoyée à l'administrateur réseau, ou une vitesse affectée à un paquet peut limiter les restrictions de transfert. Les options sont les suivantes :

- **Permit.** Achemine les paquets qui correspondent aux critères de l'ACL.
- **Deny.** Supprime les paquets qui correspondent aux critères de l'ACL.
- **Shutdown.** Supprime les paquets qui correspondent aux critères de l'ACL et désactive le port auquel le paquet était destiné. Pour réactiver un port, utilisez l'écran Port Management.

Protocol. Crée un ACE (Access Control Event) sur la base d'un protocole spécifique.

- **Select from List.** Sélectionne, dans une liste de protocoles, celui que l'ACE peut prendre comme base. Les valeurs de champ possibles sont les suivantes :
 - **Any.** Mise en correspondance entre le protocole et tous les protocoles.
 - **EIGRP.** Indique que le protocole EIGRP (Enhanced Interior Gateway Routing Protocol) est utilisé pour le classement des flux réseau.
 - **ICMP.** Indique que le protocole ICMP (Internet Control Message Protocol) est utilisé pour le classement des flux réseau.
 - **IGMP.** Indique que le protocole IGMP (Internet Group Management Protocol) est utilisé pour le classement des flux réseau.
 - **TCP.** Indique que le protocole TCP (Transmission Control Protocol) est utilisé pour le classement des flux réseau.
 - **OSPF.** Fait correspondre le paquet au protocole OSPF (Open Shortest Path First).
 - **UDP.** Indique que le protocole UDP (User Datagram Protocol) est utilisé pour le classement des flux réseau.
- **Protocol ID To Match.** Ajoute des protocoles définis par l'utilisateur aux paquets présentant une correspondance avec l'ACE. Chaque protocole porte un numéro unique. La plage de numéros valides est comprise entre 0 et 255.

TCP Flags. Filtre les paquets via l'indicateur TCP. Les paquets filtrés sont soit transférés, soit supprimés. Le filtrage des paquets via les indicateurs TCP augmente le contrôle des paquets, ce qui accroît la sécurité réseau. Les valeurs pouvant être affectées sont les suivantes :

- **Set.** Active le filtrage des paquets via des indicateurs sélectionnés.
- **Unset.** Désactive le filtrage des paquets via des indicateurs sélectionnés.
- **Don't care.** Indique que les paquets sélectionnés n'influencent pas le processus de filtrage de paquets.

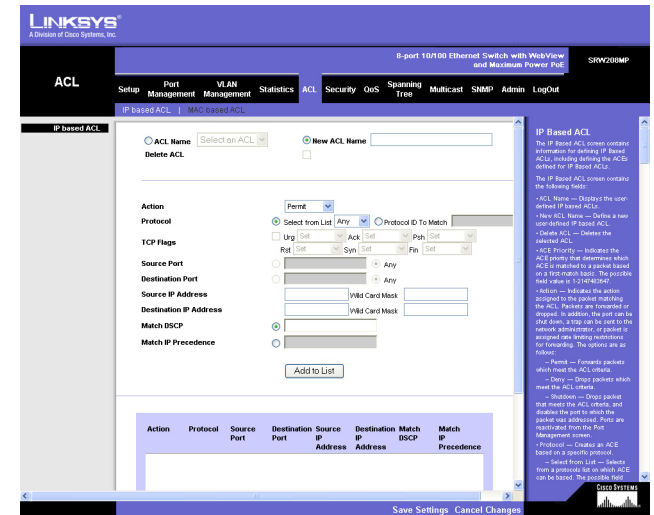


Figure 5-26 : ACL - IP Based ACL

Vous pouvez sélectionner les indicateurs TCP suivants :

Urg. Indique que le paquet est urgent.

Ack. Indique que le paquet est reconnu.

Psh. Indique que le paquet est envoyé.

Rst. Indique que la connexion a été perdue.

Syn. Indique une demande d'ouverture de session.

Fin. Indique une demande de clôture de session.

Source Port. Définit le port source TCP/UDP auquel l'ACE correspond. Ce champ n'est actif que si vous sélectionnez 800/6-TCP ou 800/17-UDP dans le menu déroulant Select from List. La plage de numéros valides est comprise entre 0 et 65535.

Destination Port. Définit le port TCP/UDP de destination. Ce champ n'est actif que si vous sélectionnez 800/6-TCP ou 800/17-UDP dans le menu déroulant Select from List. La plage de numéros valides est comprise entre 0 et 65535.

Source IP Address. Fait correspondre l'adresse IP du port source auquel les paquets sont destinés avec l'ACE.

Wildcard Mask. Définit le masque de caractères génériques de l'adresse IP source. Les masques de caractères génériques spécifient les bits utilisés et les bits ignorés. Un masque de caractères génériques 255.255.255.255 indique qu'aucun bit n'est important. Le masque de caractères génériques 0.0.0.0 indique en revanche que tous les bits sont importants. Par exemple, si l'adresse IP source est 149.36.184.198 et le masque de caractères génériques est 255.36.184.00, les huit premiers bits de l'adresse IP sont ignorés et les huit derniers sont utilisés.

Dest. IP Address. Fait correspondre l'adresse IP de destination aux paquets envoyés à l'ACE.

Wildcard Mask. Définit le masque de caractères génériques de l'adresse IP de destination.

Match DSCP. Fait correspondre la valeur DSCP du paquet avec l'ACE. Pour la mise en correspondance entre les paquets et les ACL, vous pouvez utiliser soit la valeur DSCP, soit la valeur de priorité IP. La plage valide est comprise entre 0 et 63.

Match IP Precedence. Fait correspondre la valeur de priorité IP et l'ACE. Pour la mise en correspondance entre les paquets et les ACL, vous pouvez utiliser soit la valeur DSCP, soit la valeur de priorité IP. La plage valide est comprise entre 0 et 7.

Le bouton **Add to List** permet d'ajouter les ACL basées IP configurées au tableau d'ACL basée IP, situé au bas de l'écran.

Onglet ACL - MAC Based ACL

L'écran MAC Based ACL permet de définir une ACL basée MAC. Vous ne pouvez ajouter un ACE que si l'ACL n'est pas liée à une interface.

ACL Name. Affiche les ACL basées MAC définies par l'utilisateur.

New ACL Name. Spécifie un nouveau nom d'ACL basée MAC défini par l'utilisateur.

Delete ACL. Supprime l'ACL sélectionnée.

Action. Indique l'action de transfert d'ACL. Les valeurs de champ possibles sont les suivantes :

- **Permit.** Achemine les paquets qui correspondent aux critères de l'ACL.
- **Deny.** Supprime les paquets qui correspondent aux critères de l'ACL.
- **Shutdown.** Supprime le paquet qui correspond aux critères de l'ACL et désactive le port auquel le paquet était destiné.

Source MAC Address. Fait correspondre l'adresse MAC source à laquelle les paquets sont destinés avec l'ACE.

Wildcard Mask. Définit le masque de caractères génériques de l'adresse IP source. Les masques de caractères génériques spécifient les bits utilisés et les bits ignorés. Un masque de caractères génériques 255.255.255.255 indique qu'aucun bit n'est important. Le masque de caractères génériques 0.0.0.0 indique en revanche que tous les bits sont importants. Par exemple, si l'adresse IP source est 149.36.184.198 et le masque de caractères génériques est 255.36.184.00, les huit premiers bits de l'adresse IP sont ignorés et les huit derniers sont utilisés.

Dest. MAC Address. Fait correspondre l'adresse MAC de destination à laquelle les paquets sont envoyés avec l'ACE.

Wildcard Mask. Définit le masque de caractères génériques de l'adresse IP de destination.

VLAN ID. Fait correspondre l'ID de VLAN des paquets avec l'ACE. Les valeurs de champ possibles sont comprises entre 2 et 4094.

Ether Type. Spécifie le type Ethernet des paquets.

Le bouton **Add to List** permet d'ajouter les ACL basées MAC configurées au tableau d'ACL basées MAC, situé au bas de l'écran.



Figure 5-27 : ACL - Mac Based ACL

Onglet Security - ACL Binding

Lorsqu'une ACL est liée à une interface, toutes les règles d'ACE définies sont appliquées à l'interface sélectionnée. Chaque fois qu'une ACL est affectée à un port ou LAG, les flux en provenance de cette interface ne correspondant pas à l'ACL sont mis en correspondance avec la règle par défaut (règle de suppression des paquets non concordants).

Interface. Indique l'interface à laquelle l'ACL est liée.

ACL Name. Indique l'ACL liée à l'interface.

Le bouton **Add to List** permet d'ajouter la configuration de liaison d'ACL au tableau de liaisons d'ACL, située au bas de l'écran.

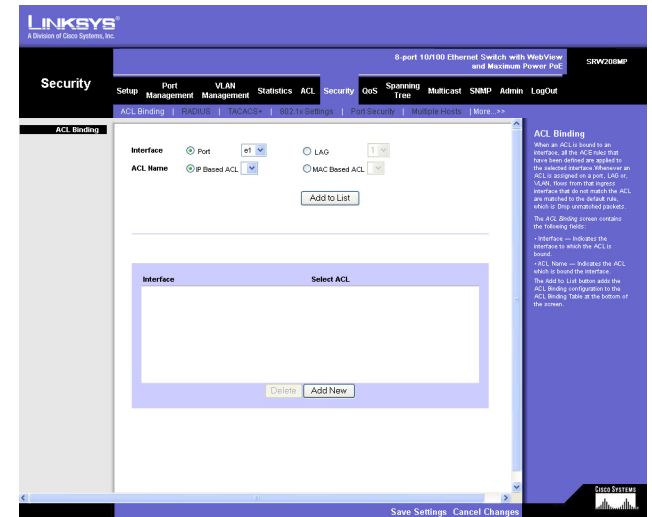


Figure 5-28 : Security - ACL Binding

Onglet Security - RADIUS

Les serveurs RADIUS (Remote Authorization Dial-In User Service) offrent une sécurité accrue sur les réseaux. Les serveurs RADIUS disposent d'une méthode d'authentification centralisée pour l'accès au Web.

IP Address. Adresse IP du serveur d'authentification.

Priority. Priorité du serveur. Les valeurs possibles sont comprises entre 0 et 65535, où 1 correspond à la valeur la plus élevée. La priorité de serveur RADIUS est utilisée pour configurer l'ordre des requêtes serveur.

Authentication Port. Identifie le port d'authentification. Le port d'authentification est utilisé pour vérifier l'authentification du serveur RADIUS. La valeur par défaut de port authentifié est 1812.

Number of Retries. Définit le nombre de requêtes transmises ayant été envoyées au serveur RADIUS avant la survenue d'une défaillance. Les valeurs possibles sont comprises entre 1 et 10. La valeur par défaut est trois.

Timeout for Reply. Définit la durée en secondes pendant laquelle le périphérique attend une réponse du serveur RADIUS avant de faire une nouvelle tentative de requête ou d'accéder au serveur suivant. Les valeurs possibles sont comprises entre 1 et 30. La valeur par défaut est trois.



Figure 5-29 : Security - RADIUS

Dead Time. Définit la durée en minutes pendant laquelle un serveur RADIUS est ignoré pour les demandes de service. La plage valide est comprise entre 0 et 2000. La valeur par défaut est de 0 minutes.

Key String. Indique la chaîne de clé par défaut utilisée pour l'authentification et le cryptage de toutes les communications RADIUS établies entre le périphérique et le serveur RADIUS. Cette clé doit correspondre au cryptage RADIUS.

Source IP Address. Définit l'adresse IP source utilisée pour communiquer avec les serveurs RADIUS.

Usage Type. Spécifie le type d'authentification du serveur RADIUS. La valeur par défaut est Login. Les valeurs de champ possibles sont les suivantes :

- **Login.** Indique que le serveur RADIUS est utilisé pour l'authentification des noms d'utilisateur et des mots de passe.
- **802.1x.** Indique que le serveur RADIUS est utilisé pour l'authentification 802.1x.
- **All.** Indique que le serveur RADIUS est utilisé pour l'authentification des noms d'utilisateur et des mots de passe, et pour l'authentification de port 802.1x.

Le bouton **Add to List** permet d'ajouter la configuration RADIUS au tableau RADIUS situé au bas de l'écran.

Onglet Security - TACACS+

Le périphérique offre un support client TACACS+ (Terminal Access Controller Access Control System). TACACS+ offre une sécurité centralisée pour la validation des utilisateurs qui accèdent au périphérique. TACACS+ offre un système de gestion centralisée des utilisateurs, tout en maintenant une bonne cohérence avec les processus d'authentification RADIUS et autres. Le protocole TACACS+ garantit l'intégrité du réseau via des échanges de protocoles cryptés entre le périphérique et le serveur TACACS+.

Host IP Address. Affiche l'adresse IP du serveur TACACS+.

Priority. Affiche l'ordre dans lequel les serveurs TACACS+ sont utilisés. La valeur par défaut est de 0.

Source IP Address. Affiche l'adresse IP source de périphérique utilisée pour la session TACACS+ entre le périphérique et le serveur TACACS+.

Key String. Définit la clé d'authentification et de cryptage pour le serveur TACACS+. Cette clé doit correspondre à la clé de cryptage du serveur RADIUS.

Authentication Port. Affiche le numéro de port utilisé pour la session TACACS+. La valeur par défaut est 49.



Figure 5-30 : Security - TACACS+

Timeout for Reply. Affiche la durée écoulée avant l'expiration de la connexion établie entre le périphérique et le serveur TACACS+. La plage valide est comprise entre 1 et 30 secondes.

Status. Affiche l'état de la connexion établie entre le périphérique et le serveur TACACS+. Les valeurs de champ possibles sont les suivantes :

- **Connected.** Une connexion est actuellement établie entre le périphérique et le serveur TACACS+.
- **Not Connected.** Aucune connexion n'est actuellement établie entre le périphérique et le serveur TACACS+.

Single Connection. Lorsque cette option est sélectionnée, elle permet de conserver une connexion ouverte entre le périphérique et le serveur TACACS+.

Le bouton **Add to List** permet d'ajouter la configuration TACACS+ au tableau TACACS+ situé au bas de l'écran.

Onglet Security - 802.1x Settings

L'authentification de ports permet d'authentifier les utilisateurs système port par port via un serveur externe. Seuls les utilisateurs système authentifiés et autorisés peuvent transmettre et recevoir des données. Les ports sont authentifiés via le serveur RADIUS à l'aide du protocole EAP (Extensible Authentication Protocol).

Enable 802.1x. Cochez cette case pour activer l'authentification 802.1x.

Port. Indique le nom de port.

Status Port Control. Indique l'état d'autorisation du port. Les valeurs de champ possibles sont les suivantes :

- **Force-Authorized.** L'état du port contrôlé est réglé sur Force-Authorized (transférer le trafic).
- **Force-Unauthenticated.** L'état du port contrôlé est réglé sur Force-Unauthenticated (supprimer le trafic).

Enable Periodic Reauthentication. Permet d'obtenir une nouvelle authentification immédiate de port.

Setting Timer. Le bouton Setting Timer permet d'ouvrir l'écran Setting Timer, dans lequel vous pouvez configurer les ports pour la fonctionnalité 802.1x.

Écran Setting Timer

Port. Indique le nom de port.

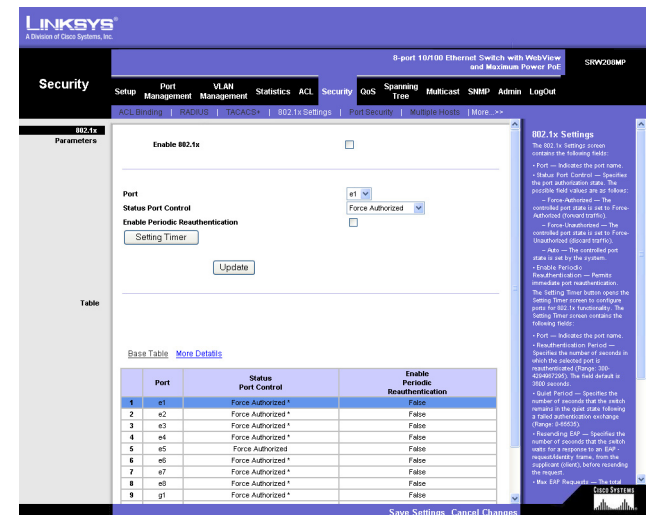


Figure 5-31 : Security - 802.1x Settings

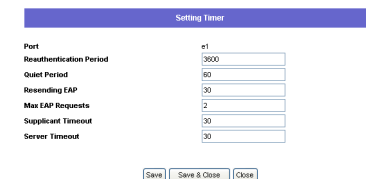


Figure 5-32 : 802.1x Settings - Setting Timer

Reauthentication Period. Indique le nombre de secondes pendant lequel le port sélectionné est à nouveau authentifié (plage : 300-4294967295). La valeur par défaut est de 3600 secondes.

Quiet Period. Indique le nombre de secondes pendant lequel le commutateur est à l'état de repos après un échec d'échange d'authentification (plage : 0-65535).

Resending EAP. Indique le nombre de secondes pendant lequel le commutateur attend une réponse à une trame de requête/d'identité EAP en provenance du client avant d'envoyer à nouveau la requête.

Max EAP Requests. Nombre total de requêtes EAP envoyées. Si aucune réponse n'est reçue pendant la période définie, le processus d'authentification est relancé. La valeur par défaut est de 2 tentatives.

Supplicant Timeout. Affiche le nombre de secondes écoulé avant que des requêtes EAP ne soient renvoyées au demandeur (plage : 1-65535). La valeur par défaut est de 30 secondes.

Server Timeout. Indique le nombre de secondes écoulé avant que le commutateur n'envoie à nouveau une requête au serveur d'authentification (plage : 1-65535). La valeur par défaut est de 30 secondes.

Onglet Security - Port Security

La sécurité réseau peut être augmentée grâce à la limitation, sur un port spécifique, de l'accès aux seuls utilisateurs disposant d'adresses MAC spécifiques. Les adresses MAC peuvent être apprises ou enregistrées dynamiquement ou configurées de façon statique. La sécurité des ports verrouillés surveille à la fois les paquets reçus et appris acheminés sur des ports spécifiques. L'accès aux ports verrouillés est limité aux utilisateurs possédant des adresses MAC spécifiques. Ces adresses sont soit définies manuellement sur le port, soit apprises sur le port jusqu'au point de verrouillage. Lorsqu'un paquet est reçu sur un port verrouillé et que l'adresse MAC source du paquet n'est pas liée à ce port (elle a été apprise sur un port différent ou est inconnue du système), le mécanisme de protection est activé et peut utiliser plusieurs options. Les paquets non autorisés arrivant sur un port verrouillé sont soit :

- Acheminés
- Éliminés sans interception
- Éliminés avec interception
- À l'origine de l'arrêt du port.

La sécurité des ports verrouillés permet également de stocker une liste d'adresses MAC dans le fichier de configuration. La liste d'adresses MAC peut être restaurée après la réinitialisation du périphérique.

Les ports désactivés sont activés à partir de la page Port Security.

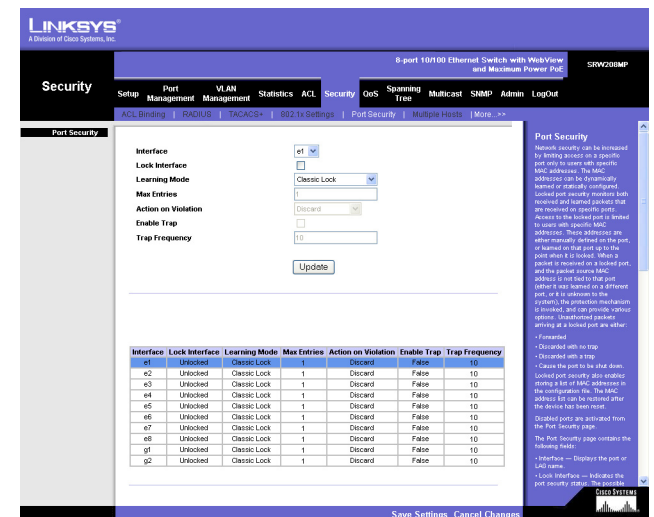


Figure 5-33 : Security - Port Security

Interface. Affiche le nom de port ou de LAG.

Lock Interface. Si vous sélectionnez cette option, l'interface spécifiée est verrouillée.

Learning Mode. Définit le type de port verrouillé. Le champ Learning Mode n'est activé que si la valeur Locked est sélectionnée dans le champ Interface Status. Les valeurs possibles sont les suivantes :

- **Classic Lock.** Verrouille le port à l'aide du mécanisme classique de verrouillage. Le port est immédiatement verrouillé, quel que soit le nombre d'adresses déjà apprises.
- **Limited Dynamic Lock.** Verrouille le port en supprimant les adresses MAC dynamiques actuellement associées au port. Le port apprend ou enregistre au maximum le nombre maximal d'adresses autorisées sur le port. Les opérations de réapprentissage et de mise à niveau d'adresses MAC sont toutes deux activées.

Pour que vous puissiez modifier le mode d'apprentissage, l'interface de verrouillage doit être configurée sur Unlocked. Une fois le mode modifié, l'interface de verrouillage peut être relancée.

Max Entries. Indique le nombre d'adresses MAC pouvant être apprises sur le port. Le champ Max Entries n'est activé que si la valeur Locked est sélectionnée dans le champ Interface Status. En outre, le mode de verrouillage dynamique limité doit être sélectionné. La valeur par défaut est de 1.

Action on Violation. Indique l'action à appliquer aux paquets qui sont acheminés vers un port verrouillé. Les valeurs de champ possibles sont les suivantes :

- **Discard.** Élimine les paquets en provenance d'une source non apprise. Il s'agit de la valeur par défaut.
- **Forward Normal.** Achemine les paquets en provenance d'une source inconnue sans apprendre l'adresse MAC.
- **Discard Disable.** Élimine les paquets en provenance d'une source inconnue et ferme le port. Le port reste fermé jusqu'à ce qu'il soit réactivé ou jusqu'à ce que le périphérique soit réinitialisé.

Enable Trap. Active les interceptions lorsqu'un paquet est reçu sur un port verrouillé.

Trap Frequency. Durée (exprimée en secondes) entre les interceptions. La valeur par défaut est de 10 secondes.

Onglet Security - Multiple Hosts

L'écran Multiple Hosts permet aux gestionnaires réseau de configurer une authentification de ports avancée pour des ports et des VLAN spécifiques.

Port. Affiche le numéro de port pour lequel l'authentification de ports avancée est activée.

Enable Multiple Hosts. Si vous cochez cette case, indique que plusieurs hôtes sont activés. Vous pouvez activer plusieurs hôtes pour désactiver le filtre d'entrée ou pour utiliser la sécurité de verrouillage de ports sur le port sélectionné.

Action on Violation. Définit l'action à appliquer aux paquets acheminés en mode hôte unique, en provenance d'un hôte dont l'adresse MAC ne correspond pas à l'adresse MAC du demandeur. Les valeurs de champ possibles sont les suivantes :

- **Discard.** Élimine les paquets. Il s'agit de la valeur par défaut.
- **Forward.** Achemine le paquet.
- **Discard Disable.** Élimine les paquets et ferme le port. Le port reste fermé jusqu'à ce qu'il soit réactivé ou jusqu'à ce que le périphérique soit réinitialisé.

Enable Traps. Si cette case est cochée, indique que des interceptions sont activées pour des hôtes multiples.

Trap Frequency. Définit la période pendant laquelle des interceptions sont envoyées à l'hôte. Le champ Trap Frequency (1-1000000) ne peut être défini que si les hôtes multiples sont désactivés. La valeur par défaut est de 10 secondes.

Status. Indique le statut de l'hôte. Si un astérisque (*) est affiché, cela signifie que le port n'est pas lié ou qu'il est fermé. Les valeurs de champ possibles sont les suivantes :

Number of Violations. Indique le nombre de paquets parvenus à l'interface en mode hôte unique, en provenance d'un hôte dont l'adresse MAC ne correspond pas à l'adresse MAC du demandeur.

Onglet Security - Storm Control

Port. Affiche le numéro de port pour lequel le contrôle d'avalanche est activé.

Broadcast Control. Indique si les types de paquets de diffusion sont transférés sur l'interface spécifique.

Mode. Indique le mode de diffusion actuellement activé sur le périphérique. Les valeurs de champ possibles sont les suivantes :

- **Unknown Unicast, Multicast & Broadcast.** Répertoire la diffusion individuelle, multidiffusion et diffusion.
- **Multicast & Broadcast.** Répertoire globalement le trafic multidiffusion et diffusion.
- **Broadcast Only.** Répertoire uniquement le trafic de diffusion.

Rate Threshold. Débit maximal (paquets par seconde) de transfert des paquets inconnus. La valeur par défaut est 3500 et la plage valide est 70 - 100000.

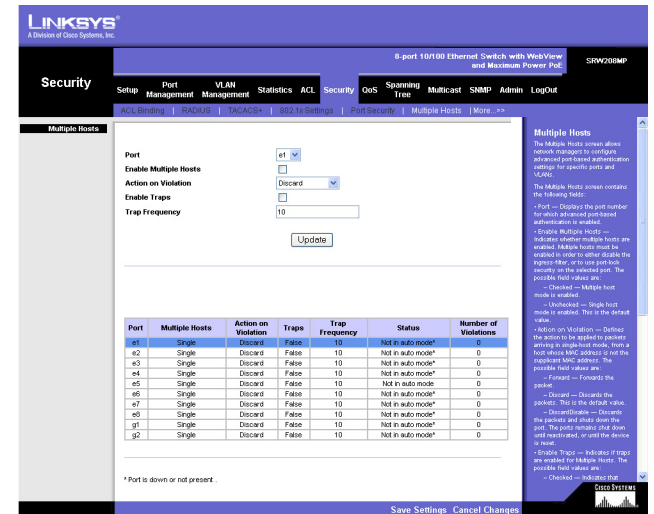


Figure 5-34 : Security - Multiple Hosts

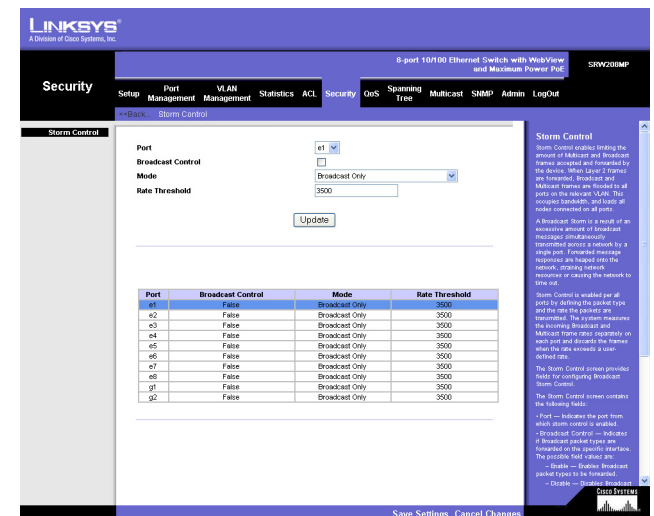


Figure 5-35 : Security - Storm Control

QoS (qualité de service)

Le trafic réseau est généralement imprévisible, et la seule assurance de base pouvant être offerte est l'optimisation des efforts de livraison du trafic. Pour relever ce défi, une qualité de service (QoS) est appliquée sur la totalité du réseau. Cela garantit que le trafic réseau possède des priorités en fonction de critères spécifiés et qu'il fait l'objet d'un traitement préférentiel. La qualité de service réseau optimise les performances réseau et s'appuie sur deux fonctions de base :

le classement du trafic entrant en classes de gestion sur la base d'un attribut, incluant :

- l'interface d'entrée,
- le contenu des paquets,
- une combinaison de ces attributs.

les méthodes de détermination de l'allocation des ressources réseau aux différentes classes, incluant :

- l'affectation du trafic réseau à une file d'attente matérielle spécifique,
- l'affectation de ressources internes,
- le profil du trafic.

Les termes classe de service (CoS) et qualité de service (QoS) sont utilisés dans le contexte suivant :

La classe de service (CoS) offre des services de trafic de couche 2. La classe de service se réfère au classement du trafic en classes de trafic, gérées comme un tout, sans paramètres par flux. Les classes de services sont généralement liées au service 802.1p qui classe les flux selon leur priorité en Couche 2, conformément aux indications de l'en-tête VLAN.

La qualité de service (QoS) se réfère au trafic de la Couche 2 et des Couches supérieures. La qualité de service gère les paramètres établis par flux, y compris au sein d'une même classe de trafic.

Onglet QoS - CoS Settings

L'écran CoS contient des champs qui permettent d'activer ou de désactiver les classes de services. Par ailleurs, vous pouvez sélectionner le mode Trust. Ce mode s'appuie sur des champs prédéfinis au sein du paquet pour déterminer les paramètres applicables à la file d'attente de sortie.

L'écran CoS Settings se compose de deux zones (CoS Settings et CoS to Queue).

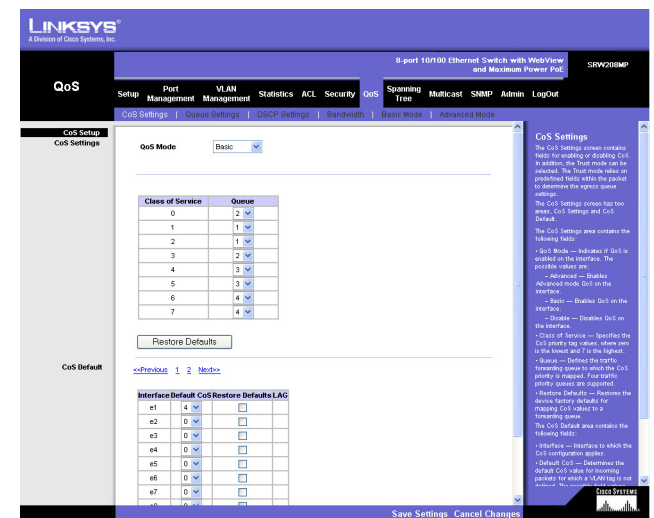


Figure 5-36 : QoS - CoS Settings

CoS Mode. Indique si la qualité de service est activée sur l'interface. Les valeurs de champ possibles sont les suivantes :

- **Disable.** Désactive la qualité de service sur l'interface.
- **Basic.** Active la qualité de service sur l'interface.
- **Advanced.** Active le mode avancé de qualité de service sur l'interface.

Class of Service. Spécifie les valeurs de priorité de classe de service (zéro représente la valeur la plus faible et 7 représente la valeur la plus élevée).

Queue. Définit la file d'attente de transfert de trafic à laquelle est mappée la priorité de classe de service. Quatre files d'attente de priorité de trafic sont prises en charge.

Le bouton **Restore Defaults** permet de restaurer les valeurs par défaut pour le mappage des valeurs CoS à une file d'attente de transfert.

CoS Default

Interface. Interface à laquelle s'applique la configuration CoS.

Default CoS. Détermine la valeur CoS par défaut applicable aux paquets entrants, pour lesquels une balise de VLAN n'est pas définie. Les valeurs possibles sont comprises dans la plage 0 - 7. La valeur CoS par défaut est de 0.

Restore Defaults. Restaure les valeurs par défaut pour le mappage des valeurs CoS à une file d'attente de transfert.

LAG. LAG auquel s'applique la configuration CoS.

Onglet QoS - Queue Settings

L'écran Queue Setting contient des champs qui permettent de définir les types de transfert de file d'attente QoS.

Strict Priority. Indique que la planification du trafic pour la file d'attente sélectionnée ne prend comme base que la priorité de la file d'attente.

WRR. Indique que la planification du trafic de la file d'attente sélectionnée ne prend comme base que le WRR.

Queue. Indique la file d'attente dont les paramètres s'affichent. La plage valide est comprise entre 1 et 4.

WRR Weight. Affiche les charges WRR aux files d'attente.

% of WRR Bandwidth. Affiche le niveau de bande passante affecté à la file d'attente. Ces valeurs sont fixes et ne sont pas définies par l'utilisateur.

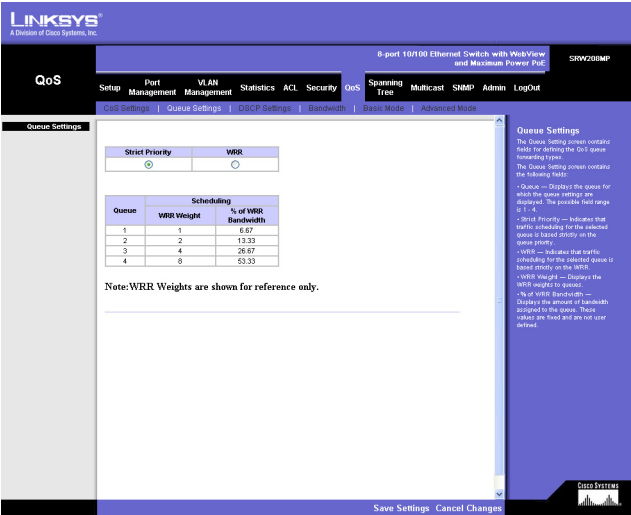


Figure 5-37 : QoS - Queue Settings

Onglet QoS - DSCP Settings

L'écran DSCP Settings permet d'activer le mappage des valeurs DSCP aux files d'attente spécifiques.

L'écran DSCP Settings contient les champs suivants :

DSCP. Indique la valeur DSCP présente dans le paquet entrant.

Queue. Mappe la valeur DSCP à la file d'attente sélectionnée.

Onglet QoS - Bandwidth

L'écran Bandwidth permet aux gestionnaires réseau de définir les paramètres de bande passante applicables à une interface de sortie spécifique. La modification de la planification de la file d'attente affecte globalement les paramètres de celle-ci. L'écran Bandwidth n'est pas utilisé avec le mode Service, car les paramètres de la bande passante prennent comme base les services.

Le profil de file d'attente peut prendre comme base les files d'attente et/ou les interfaces. Il est déterminé par la valeur la plus faible spécifiée. Vous pouvez sélectionner le type de profil de file d'attente dans l'écran Bandwidth.

Interface. Indique l'interface pour laquelle les informations de profil de file d'attente sont affichées. Les valeurs de champ possibles sont les suivantes :

- **Port.** Indique le port pour lequel les paramètres de bande passante sont affichés.
- **LAG.** Indique le LAG pour lequel les paramètres de bande passante sont affichés.

Ingress Rate Limit Status. Indique si la limitation de débit de transfert est définie sur l'interface.

Rate Limit (62-1000000 Kbps). Définit le niveau de bande passante affecté à l'interface. Les valeurs de champ possibles sont comprises entre 62 et 1 000 000 Kbits/s.

Egress Shaping Rate on Selected Port. Indique si la limitation de débit de transfert est activée sur l'interface.

Committed Information Rate (CIR). Définit le taux CIR comme étant le type de profil de file d'attente. La plage valide est comprise entre 64 et 1 000 000 Kbits/s.

Committed Burst Size (CBS). Définit la taille CBS comme étant le type de profil de file d'attente. La plage valide est comprise entre 4 096 et 16 769 020 Kbits/s. La taille CBS ne peut pas être configurée sur les ports FE.

Le bouton **Add to List** permet d'ajouter la configuration de bande passante au tableau de bandes passantes situé au bas de l'écran.

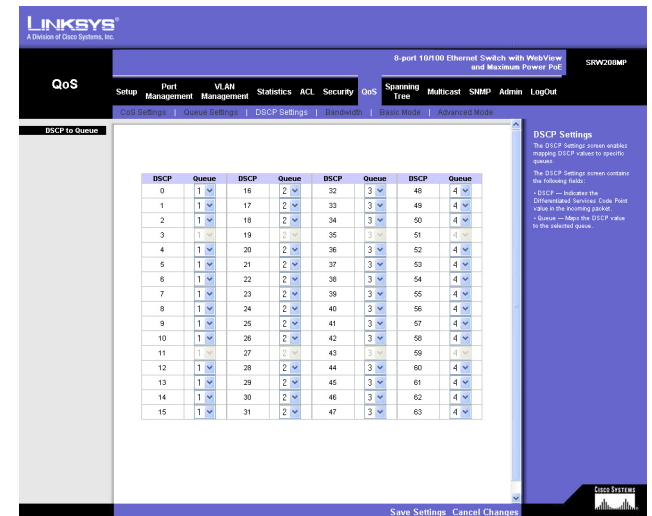


Figure 5-38 : QoS - DSCP Settings

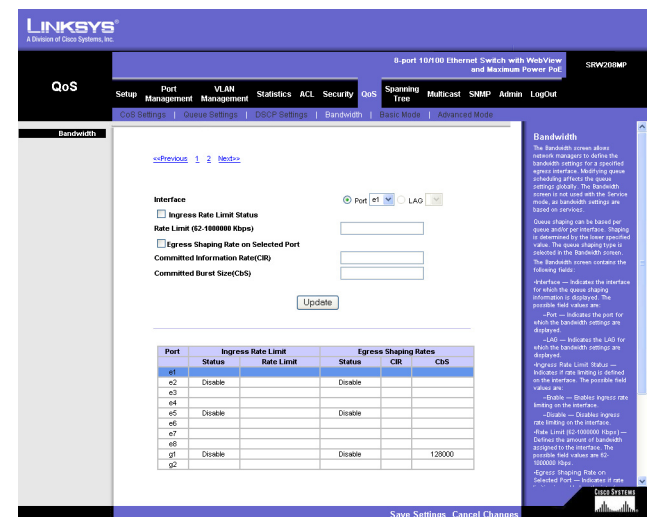


Figure 5-39 : QoS - Bandwidth

Onglet QoS - Basic Mode

L'écran Basic Mode contient les champs suivants :

Trust Mode. Affiche le mode Trust. Si la balise CoS et la balise DSCP d'un paquet sont mappées à des files d'attente différentes, ce mode détermine la file d'attente à laquelle le paquet est affecté. Les valeurs possibles sont les suivantes :

- **CoS.** Définit le mode Trust pour les classes de service sur le périphérique. Le mappage CoS détermine la file d'attente de paquets.
- **DSCP.** Définit la valeur DSCP pour le mode Trust sur le périphérique. Le mappage DSCP détermine la file d'attente de paquets.

Onglet QoS - Advanced Mode

Le mode QoS avancé contient des règles de spécification de classement de flux et inclut l'affectation d'actions de règles de gestion de bande passante. Ces règles prennent comme base les listes de contrôle d'accès (voir l'onglet Access Control).

Les ACL basées MAC et les ACL basées IP peuvent être regroupées en structures plus complexes appelées stratégies. Les stratégies peuvent s'appliquer à une interface. Les ACL correspondantes sont appliquées à la séquence dans laquelle elles apparaissent au sein de la stratégie. Une seule stratégie peut être associée à un port.

En mode QoS avancé, les ACL peuvent être appliquées directement à une interface dans Security - ACL Binding. Toutefois, une stratégie et une ACL ne peuvent pas être appliquées simultanément à une interface.

Après avoir affecté des paquets à une file d'attente spécifique, les services tels que la configuration de files d'attente de sortie pour la planification ou le profil de configuration de sortie pour la taille de rafale de données, le CIR ou le CBS par interface ou par file d'attente peuvent être appliqués.

Out of Profile DSCP Assignments. Ce bouton permet d'ouvrir l'écran Out of Profile DSCP.

Écran Out of Profile DSCP

DSCP In. Affiche la valeur DSCP In.

DSCP Out. Affiche la valeur DSCP Out actuelle. Vous pouvez sélectionner une nouvelle valeur dans le menu déroulant.

Le bouton **Policy Settings** permet d'ouvrir l'écran Policy Name.



Figure 5-40 : QoS - Basic Mode

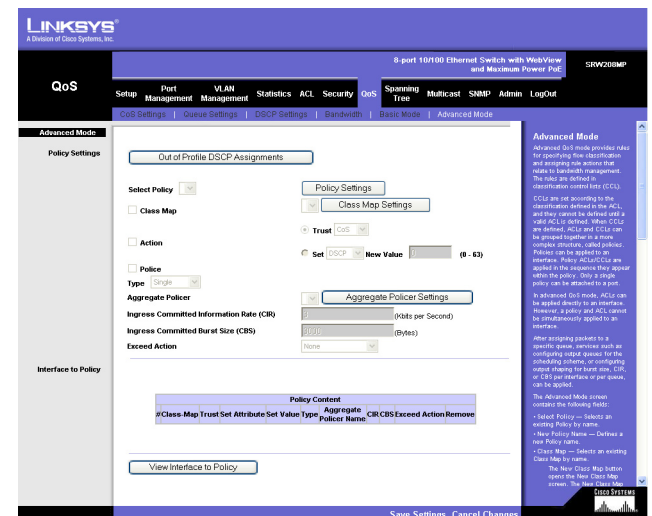


Figure 5-41 : QoS - Advanced Mode

Écran Policy Name

Policy Name. Définit un nouveau nom de stratégie.

Add to List. Le bouton Add to List permet d'ajouter la stratégie au tableau de noms de stratégies.

Select Policy. Permet de sélectionner une stratégie existante en sélectionnant son nom. La stratégie peut se composer des éléments suivants :

- Class Map
- Action
- Policer

New Policy Name. Définit un nouveau nom de stratégie.

Class Map. Permet de sélectionner un nom existant de mappage de classes.

New Class Map. Le bouton New Class Map permet d'ouvrir l'écran New Class Map.

Écran New Class Map.

Class Map Name. Définit un nouveau nom de mappage de classes.

Preferred ACL. Indique si les paquets correspondent en priorité à une ACL basée IP ou à une ACL basée MAC. Les valeurs de champ possibles sont les suivantes :

- **IP Based ACLs.** Fait correspondre les paquets en priorité à des ACL basées IP, puis à des ACL basées MAC.
- **MAC Based ACLs.** Fait correspondre les paquets en priorité à des ACL basées MAC, puis à des ACL basées IP.

IP ACL. Fait correspondre les paquets en priorité à des ACL basées IP, puis à des ACL basées MAC.

Match. Critères utilisés pour la correspondance entre les adresses IP et/ou MAC et l'adresse d'une ACL. Les valeurs possibles sont les suivantes :

- **And.** Les ACL basées MAC et IP doivent correspondre à un paquet.
- **Or.** Les ACL basées MAC ou IP doivent correspondre à un paquet.

MAC ACL. Fait correspondre les paquets en priorité à des ACL basées MAC, puis à des ACL basées IP.

Police. Active la fonctionnalité Policer.

Type. Type de responsable de stratégie pour cette classe. Les valeurs possibles sont les suivantes :

DSCP Map															
DSCP In	DSCP Out	DSCP In	DSCP Out	DSCP In	DSCP Out	DSCP In	DSCP Out	DSCP In	DSCP Out	DSCP In	DSCP Out	DSCP In	DSCP Out	DSCP In	DSCP Out
0	0	16	16	32	32	48	48								
1	1	17	17	33	33	49	49								
2	2	18	18	34	34	50	50								
3	3	19	19	35	35	51	51								
4	4	20	20	36	36	52	52								
5	5	21	21	37	37	53	53								
6	6	22	22	38	38	54	54								
7	7	23	23	39	39	55	55								
8	8	24	24	40	40	56	56								
9	9	25	25	41	41	57	57								
10	10	26	26	42	42	58	58								
11	11	27	27	43	43	59	59								
12	12	28	28	44	44	60	60								
13	13	29	29	45	45	61	61								
14	14	30	30	46	46	62	62								
15	15	31	31	47	47	63	63								

Figure 5-42 : Advanced Mode - Out of Profile DSCP

Policy Name

Policy Name

Add to List

Policy Name

Delete

Cancel

Save

Save & Close

Close

Figure 5-43 : Advanced Mode - Policy Name

New Class Map

Add Class Map

Class Map Name

Preferred ACL

IP Based

Match

Or

MAC ACL

Add to List

#

Class Map Name

Preferred ACL

IP ACL

Match

MAC ACL

Delete

Cancel

Save

Save & Close

Close

Figure 5-44 : Advanced Mode - New Class Map

Aggregate Policer. Configure la classe de façon à utiliser un responsable de stratégie global configuré, sélectionné dans le menu déroulant. Un responsable de stratégie global est défini si le responsable de stratégie est partagé entre plusieurs classes. Le trafic provenant de deux ports différents peut être configuré à des fins de stratégie. Un responsable de stratégie global peut s'appliquer à plusieurs classes au sein de la même mappe, mais ne peut pas être utilisé dans des mappes différentes.

Single. Configure la classe afin d'utiliser des informations et des actions configurées manuellement.

Aggregate Policer. Responsables de stratégie définis par l'utilisateur.

Paramètres Aggregate Policer. Le bouton Aggregate Policer permet d'ouvrir l'écran New Aggregate Policer.

Écran New Aggregate Policer

Aggregate Policer Name. Saisissez un nom dans ce champ.

Ingress Committed Information Rate (CIR). Définit le CIR, exprimé en bits par seconde. Ce champ ne doit être utilisé que lorsque la valeur affectée au champ Police est Single.

Ingress Committed Burst Size (CBS). Définit le CBS en octets par seconde. Ce champ ne doit être utilisé que lorsque la valeur affectée au champ Police est Single.

Exceed Action. L'action affectée aux paquets entrants dépasse la valeur de CIR. Ce champ ne doit être utilisé que lorsque la valeur affectée au champ Police est Single. Les valeurs possibles sont les suivantes :

- **Drop.** Supprime les paquets qui dépassent la valeur CIR définie.
- **Remark DSCP.** Signale les valeurs DSCP de paquets excédant la valeur CIR définie.
- **None.** Achemine les paquets dépassant la valeur CIR définie.

Spanning Tree

Le protocole STP (Spanning Tree Protocol) contient une topologie adaptée à la disposition de ponts. Ce protocole contient également un chemin entre les stations finales d'un réseau, ce qui permet d'éliminer les boucles.

Les boucles apparaissent lorsque des routes différentes existent entre des hôtes. Les boucles d'un réseau étendu peuvent utiliser des ponts pour acheminer indéfiniment le trafic, ce qui augmente ce dernier et diminue l'efficacité du réseau.

Le périphérique prend en charge les versions de Spanning Tree suivantes :

Figure 5-45 : Advanced Mode - New Aggregate Policer

- **Classic STP.** Offre un chemin unique entre stations finales, évitant ainsi les boucles.
- **Rapid STP.** Détecte et utilise les topologies réseau qui offrent une convergence plus rapide d'arborescence, sans créer de boucles de transmission.
- **Multiple STP.** Offre une connectivité totale pour les paquets alloués à un réseau VLAN. L'option Multiple STP prend comme base le protocole RSTP. En outre, l'option Multiple STP transfère des paquets affectés à différents réseaux VLAN via différentes régions MST. Les régions MST jouent le rôle de pont.

Onglet Spanning Tree - STP Status

L'écran STP Status décrit le statut STP sur le périphérique.

Spanning Tree State. Indique si le protocole STP est activé sur le périphérique.

Spanning Tree Mode. Indique le mode STP via lequel le protocole STP est activé sur le périphérique.

Bridge ID. Identifie la priorité de pont et l'adresse MAC.

Designated Root. Indique l'ID du pont présentant le coût de chemin le plus faible jusqu'à l'ID d'instance.

Root Port. Indique le numéro de port offrant le coût de chemin le moins élevé entre ce pont et le pont racine. Cet aspect est d'autant plus important que le pont n'est pas la racine. La valeur par défaut est de zéro.

Root Path Cost. Coût du chemin entre ce pont et la racine.

Root Maximum Age (sec). Indique la valeur Maximum Age Time pour le périphérique. La durée maximale d'attente d'envoi indique la durée, exprimée en secondes, pendant laquelle un pont est en attente d'envoi de messages de configuration. La valeur par défaut de cette option est de 20 secondes. La plage valide est comprise entre 6 et 40 secondes.

Root Hello Time (sec). Indique la durée d'attente du périphérique. La durée d'attente indique la durée, en secondes, pendant laquelle un pont racine est en attente entre deux messages de configuration. La valeur par défaut est de 2 secondes. La plage valide est comprise entre 1 et 10 secondes.

Root Forward delay (sec). Indique la durée de retard d'envoi du périphérique. La durée de retard d'envoi indique la durée, en secondes, pendant laquelle un pont est à l'état d'écoute avant l'envoi de paquets. La valeur par défaut est de 15 secondes. La plage valide est comprise entre 4 et 30 secondes.

Topology Changes Counts. Indique le nombre total de modifications d'état STP.

Last Topology Change. Indique la durée écoulée depuis l'initialisation ou la réinitialisation du pont, ainsi que la dernière modification topographique apportée. Cette durée s'affiche au format jour heure minute seconde (2 jours 5 heures 10 minutes et 4 secondes, par exemple).

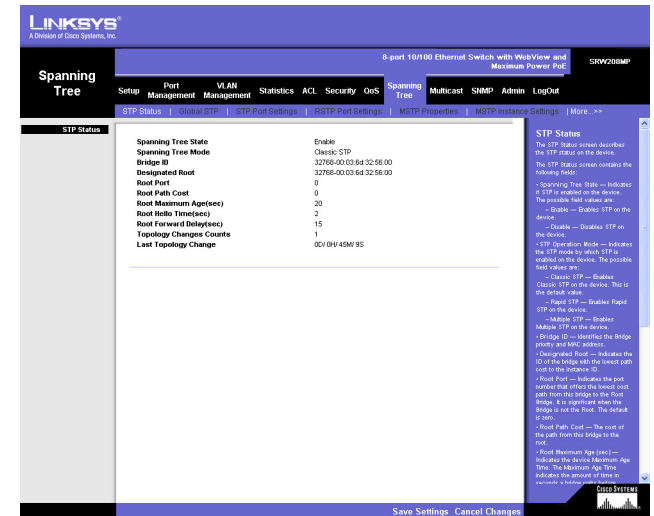


Figure 5-46 : Spanning Tree - STP Status

Onglet Spanning Tree - Global STP

L'écran Global STP contient des paramètres permettant d'activer le protocole STP sur le périphérique.

Global Setting

Spanning Tree State. Indique si le protocole STP est activé sur le périphérique.

STP Operation Mode. Indique le mode STP via lequel le protocole STP est activé sur le périphérique. Les valeurs de champ possibles sont les suivantes :

- **Classic STP.** Active Classic STP sur le périphérique. Il s'agit de la valeur par défaut.
- **Rapid STP.** Active Rapid STP sur le périphérique.
- **Multiple STP.** Active Multiple STP sur le périphérique.

BPDU Handling. Détermine le mode de gestion des paquets BPDU lorsque le protocole STP est désactivé sur le port/périphérique. Les BPDU sont utilisés pour la transmission d'informations sur l'arborescence étendue (spanning tree). Les valeurs de champ possibles sont les suivantes :

- **Filtering.** Filtre les paquets BPDU lorsque l'arborescence étendue est désactivée sur une interface. Il s'agit de la valeur par défaut.
- **Flooding.** Filtre les paquets BPDU lorsque l'arborescence étendue est désactivée sur une interface.

Path Cost Default Values. Spécifie la méthode utilisée pour l'affectation de coûts de chemin par défaut aux ports STP. Les valeurs de champ possibles sont les suivantes :

- **Short.** Indique la plage 1 à 65535 pour les coûts de chemin de ports. Il s'agit de la valeur par défaut.
- **Long.** Indique la plage 1 à 200000000 pour les coûts de chemin de ports. Les coûts par défaut affectés à une interface varient en fonction de la méthode sélectionnée.

Bridge Settings

Priority. Indique la valeur de priorité de pont. Lorsque des commutateurs ou des ponts utilisent STP, une priorité est affectée à chacun d'entre eux. Après l'échange des BPDU, le périphérique portant la priorité la moins élevée devient le pont racine. La valeur par défaut est 32768. La valeur de priorité de port est exprimée par incréments de 4 096 (par exemple, 4096, 8192, 12288, etc.). La plage valide est comprise entre 0 et 65535.

Hello Time. Indique la durée d'attente du périphérique. La durée d'attente indique la durée, en secondes, pendant laquelle un pont racine est en attente entre deux messages de configuration. La valeur par défaut est de 2 secondes. La plage valide est comprise entre 1 et 10 secondes.



Figure 5-47 : Spanning Tree - Global STP

Max Age. Indique la durée maximale d'attente d'envoi observée par le périphérique. La durée maximale d'attente d'envoi indique la durée, exprimée en secondes, pendant laquelle un pont est en attente d'envoi de messages de configuration. La valeur par défaut de cette option est de 20 secondes. La plage valide est comprise entre 6 et 40 secondes.

Forward Delay. Indique la durée de retard d'envoi du périphérique. La durée de retard d'envoi indique la durée, en secondes, pendant laquelle un pont est à l'état d'écoute avant l'envoi de paquets. La valeur par défaut est de 15 secondes. La plage valide est comprise entre 4 et 30 secondes.

Onglet Spanning Tree - STP Port Settings

Les administrateurs réseau peuvent affecter des paramètres STP à des interfaces spécifiques à l'aide de l'écran STP Interface Settings.

L'écran STP Interface Settings contient les champs suivants :

Interface. Indique le port ou le LAG sur lequel STP est activé.

STP. Indique si STP est activé sur le port.

Port Fast. Indique si Fast Link est activé sur le port. Si le mode Fast Link est activé sur un port, le port est automatiquement à l'état de transfert lorsque la liaison du port est active. Fast Link optimise la convergence de protocole STP. La convergence STP peut durer 30 à 60 secondes sur les réseaux étendus.

Port State. Affiche l'état STP actuel d'un port. S'il est activé, l'état du port détermine l'action de transfert de trafic. Les différents états de port admis sont les suivants :

- **Disabled.** Indique que STP est actuellement désactivé sur le port. Le port achemine le trafic tout en apprenant les adresses MAC.
- **Blocking.** Indique que le port est actuellement bloqué et ne peut pas acheminer le trafic ou apprendre les adresses MAC. Le blocage est affiché lorsque l'option Classic STP est activée.
- **Listening.** Indique que le port est en mode d'écoute. Le port ne peut pas acheminer le trafic, ni apprendre les adresses MAC.
- **Learning.** Indique que le port est en mode d'apprentissage. Le port ne peut pas acheminer le trafic, mais il peut apprendre de nouvelles adresses MAC.
- **Forwarding.** Indique que le port est en mode de transfert. Le port peut acheminer le trafic et apprendre de nouvelles adresses MAC.



Figure 5-48 : Spanning Tree - STP Port Settings

Speed. Indique la vitesse à laquelle le port fonctionne.

Path Cost. Indique la contribution du port au coût de chemin racine. Ce coût est ajusté à la hausse ou à la baisse et est utilisé pour l'acheminement du trafic en cas de reroutage d'un chemin.

Default Path Cost. Si vous sélectionnez cette option, le coût de chemin par défaut est utilisé.

Priority. Valeur de priorité du port. La valeur de priorité influence le choix du port lorsqu'un pont possède deux ports connectés au sein d'une boucle. Cette valeur est comprise entre 0 et 240. La valeur de priorité s'exprime par incréments de 16.

Designated Bridge ID. Indique la priorité de pont et l'adresse MAC du pont désigné.

Designated Port ID. Indique la priorité et l'interface du port sélectionné.

Designated Cost. Indique le coût du port participant à la topologie STP. Les ports affichant un coût peu élevé sont moins exposés aux blocages en cas de boucles détectées par STP.

Forward Transitions. Indique le nombre de fois où le port est passé de l'état de blocage à l'état de transfert.

Onglet Spanning Tree - RSTP Port Settings

Alors que l'arborescence étendue classique empêche le transfert de boucles (Couche 2) au sein d'une topologie réseau générale, la convergence peut durer 30 à 60 secondes. Cela peut retarder la détection d'éventuelles boucles et la propagation des modifications d'état apportées à la topologie. Le protocole RSTP (Rapid Spanning Tree Protocol) détecte et utilise des topologies réseau qui permettent d'obtenir une convergence STP plus rapide sans création de boucles de transfert.

Interface. Affiche le port ou le LAG sur lequel le protocole Rapid STP est activé.

Role. Indique le rôle de port affecté par l'algorithme STP pour les chemins STP. Les valeurs de champ possibles sont les suivantes :

- **Root.** Indique le coût de chemin le moins élevé pour le transfert des paquets au commutateur racine.
- **Designated.** Indique le port ou le LAG via lequel le commutateur désigné est connecté au réseau LAN.
- **Alternate.** Indique un autre chemin vers le commutateur racine à partir de l'interface racine.

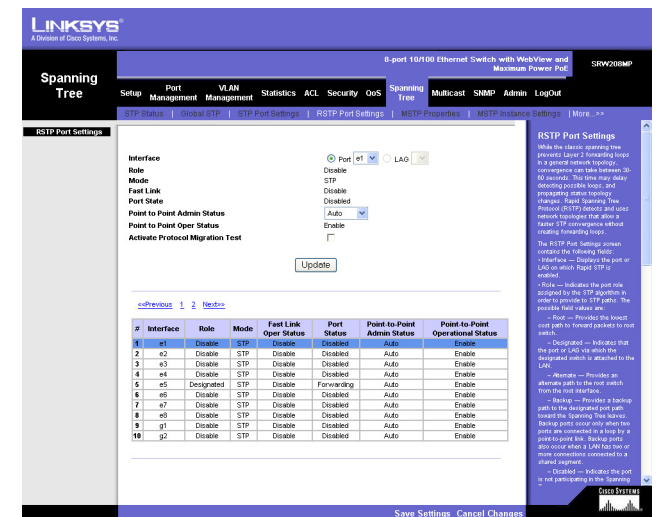


Figure 5-49 : Spanning Tree - RSTP Port Settings

- **Backup.** Indique un autre chemin de sauvegarde que le chemin de port désigné, via les feuilles Spanning Tree. Ces ports de sauvegarde ne sont indiqués que lorsque deux ports sont connectés au sein d'une boucle par une liaison point à point. Ils sont également présents lorsqu'une ou plusieurs connexions sont établies avec un segment partagé, au sein d'un réseau LAN.
- **Disabled.** Indique que le port ne participe pas au Spanning Tree.

Mode. Indique le mode Spanning Tree en cours d'utilisation. Le mode Spanning Tree peut être sélectionné dans l'écran Global STP. Les valeurs de champ possibles sont les suivantes :

- **Classic STP.** Indique que Classic STP est activé sur le périphérique.
- **Rapid STP.** Indique que Rapid STP est activé sur le périphérique.
- **Multiple STP.** Indique que Multiple STP est activé sur le périphérique.

Fast Link. Indique si Fast Link est activé ou désactivé pour le port ou le LAG. Si Fast Link est activé pour un port, celui-ci passe automatiquement à l'état de transfert.

Port State. Indique si RSTP est activé sur l'interface.

Point-to-Point Admin Status. Indique si des liaisons point à point sont établies, ou autorise le périphérique à en établir une. Les valeurs de champ possibles sont les suivantes :

- **Auto.** Les liaisons point à point sont automatiquement établies par le périphérique.
- **Enabled.** Active l'établissement de liaisons point à point par le périphérique. Pour établir des communications sur une liaison point à point, le protocole PPP d'origine envoie tout d'abord des paquets LCP (Link Control Protocol) afin de configurer et de tester la liaison de données. Une fois qu'une liaison a été établie et que des applications facultatives ont été négociées en fonction des besoins du protocole LCP, le protocole PPP d'origine envoie des paquets NCP (Network Control Protocols) pour sélectionner et configurer un ou plusieurs protocoles de couche réseau. Une fois que chaque protocole de couche réseau sélectionné a été configuré, les paquets de chacun de ces protocoles peuvent être envoyés via cette liaison. La liaison reste configurée pour les communications jusqu'à ce que des paquets LCP ou NCP explicites ferment la liaison, ou jusqu'à ce qu'un événement extérieur survienne. Il s'agit du type de liaison de port de commutateur réel. Il peut être différent de l'état administratif.
- **Disabled.** Désactive la liaison point à point.

Point-to-Point Oper Status. Indique l'état de fonctionnement point à point.

Pour exécuter un test de migration, appuyez sur Activate en regard du champ Activate Protocol Migration Test. Le test envoie des paquets LCP (Link Control Protocol) pour déterminer si une liaison de données est activée.

Onglet Spanning Tree - MSTP Properties

MSTP présente différents scénarii d'équilibrage de charge. Par exemple, si le port A est bloqué dans une instance STP, le même port passe à l'état de transfert dans une autre instance STP. L'écran MSTP Properties contient des informations permettant de définir les paramètres MSTP globaux (noms de régions, révisions MSTP et nombre maximal de tronçons).

L'écran MSTP Properties contient les champs suivants :

Region Name. Indique un nom de région STP défini par l'utilisateur.

Revision. Définit le numéro 16 bits qui identifie la révision de la configuration MST en cours. Le numéro de révision est requis dans la configuration MST. La plage valide est comprise entre 0 et 65535.

Max Hops. Indique le nombre total de tronçons d'une région spécifique avant la suppression du BPDU. Une fois le BPDU supprimé, les informations sur le port expirent. La plage valide est comprise entre 1 et 40. La valeur par défaut est de 20 tronçons.

IST Master. Permet d'identifier l'instance maître Spanning Tree. Elle représente la racine de l'instance spécifiée.

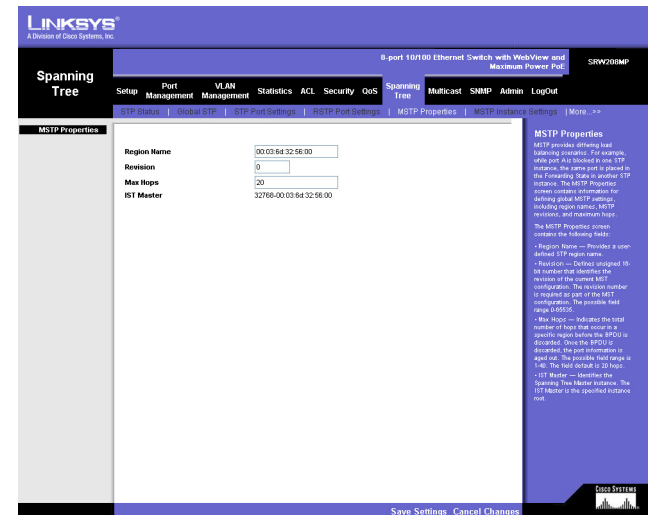


Figure 5-50 : Spanning Tree - MSTP Properties

Onglet Spanning Tree - MSTP Instance Settings

Le fonctionnement de MSTP effectue des mappages entre des réseaux VLAN et des instances STP. Les paquets affectés à des réseaux VLAN sont transmis via différents chemins au sein de régions MST (Multiple Spanning Trees). Les régions représentent un ou plusieurs ponts MST permettant de transférer des trames. Au cours de la configuration de MST, la région MST à laquelle le périphérique appartient est définie. Une configuration se compose du nom, de la révision et de la région auxquels le périphérique appartient.

Les administrateurs réseau peuvent configurer des instances MSTP dans l'écran MSTP Instance Settings.

Instance ID. Définit le groupe VLAN auquel l'interface est affectée.

Included VLAN. Permet de mapper le réseau VLAN sélectionné à l'instance sélectionnée. Chaque réseau VLAN appartient à une instance.

Bridge Priority. Indique la priorité applicable au périphérique d'instance Spanning Tree sélectionné. La plage valide est comprise entre 0 et 61440.

Designated Root Bridge ID. Indique l'ID du pont présentant le coût de chemin le plus faible jusqu'à l'ID d'instance.

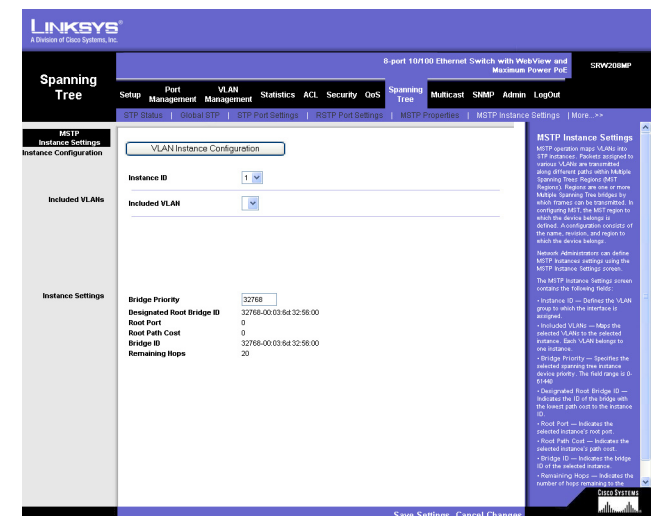


Figure 5-51 : Spanning Tree - MSTP Instance Settings

Root Port. Indique le port racine de l'instance sélectionnée.

Root Path Cost. Indique le coût de chemin de l'instance sélectionnée.

Bridge ID. Indique l'ID de pont de l'instance sélectionnée.

Remaining Hops. Indique le nombre de tronçons restant à franchir jusqu'à la destination suivante.

Onglet Spanning Tree - MSTP Interface Settings

Les administrateurs réseau peuvent affecter des paramètres d'interface MSTP via l'écran MSTP Interface Settings.

L'écran MSTP Interface Settings contient les champs suivants :

Instance ID. Répertorie les instances MSTP configurées sur le périphérique. La plage valide est comprise entre 0 et 15.

Interface. Indique l'interface pour laquelle les paramètres MSTP sont affichés. Les valeurs de champ possibles sont les suivantes :

- **Port.** Indique le port pour lequel les paramètres MSTP sont affichés.
- **LAG.** Indique le LAG pour lequel les paramètres MSTP sont affichés.

Port State. Indique si le port est activé pour l'instance spécifique.

Type. Indique si le port est un port point à point ou un port connecté à un concentrateur. Les valeurs de champ possibles sont les suivantes :

- **Boundary Port.** Indique que le port est un port frontière. Un port frontière relie des ponts MST à un réseau LAN au sein d'une région périphérique. Si le port est un port frontière, cela permet également d'indiquer si le périphérique situé à l'autre extrémité de la liaison fonctionne en mode RSTP ou STP.
- **Master Port.** Indique que le port est un port maître. Un port maître permet d'obtenir une connectivité entre une région MSTP et la racine CIST périphérique.
- **Internal.** Indique que le port est un port interne.

Role. Indique le rôle de port affecté par l'algorithme STP pour les chemins STP. Les valeurs de champ possibles sont les suivantes :

- **Root.** Indique le chemin dont le coût est le moins élevé pour l'acheminement de paquets à destination du périphérique racine.
- **Designated.** Indique le port ou le LAG via lequel le périphérique désigné est connecté au réseau LAN.

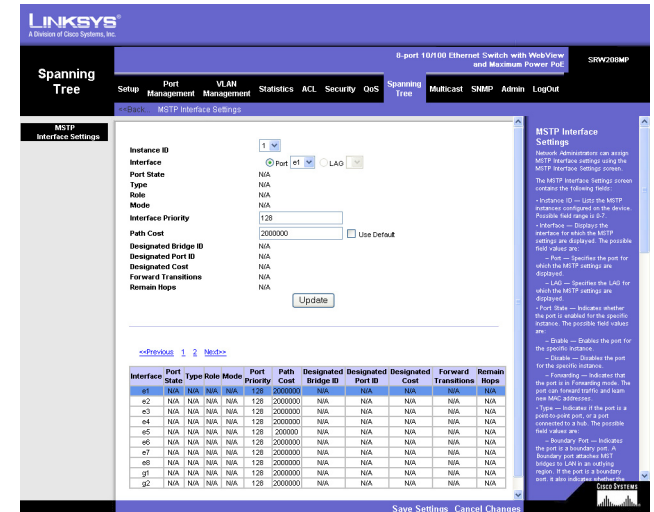


Figure 5-52 : Spanning Tree - MSTP Interface Settings

- **Alternate.** Indique un autre chemin vers le périphérique racine à partir de l'interface racine.
- **Backup.** Indique un autre chemin de sauvegarde que le chemin de port désigné, via les feuilles Spanning Tree. Ces ports de sauvegarde ne sont indiqués que lorsque deux ports sont connectés au sein d'une boucle par une liaison point à point. Ils sont également présents lorsqu'une ou plusieurs connexions sont établies avec un segment partagé, au sein d'un réseau LAN.
- **Disabled.** Indique que le port ne participe pas au Spanning Tree.

Mode. Indique le mode Spanning Tree en cours d'utilisation. Le mode Spanning Tree peut être sélectionné dans l'écran Global STP. Les valeurs de champ possibles sont les suivantes :

- **Classic STP.** Indique que Classic STP est activé sur le périphérique.
- **Rapid STP.** Indique que Rapid STP est activé sur le périphérique.
- **Multiple STP.** Indique que Multiple STP est activé sur le périphérique.

Interface Priority. Définit la priorité d'interface pour l'instance spécifiée. La valeur par défaut est de 128.

Path Cost. Indique la contribution du port à l'instance Spanning Tree. La plage autorisée est comprise entre 1 et 200000000.

Designated Bridge ID. Indique l'ID de pont reliant la liaison ou le réseau LAN partagé à la racine.

Designated Port ID. Indique l'ID du pont désigné reliant la liaison ou le réseau LAN partagé à la racine.

Designated Cost. Indique que le coût de chemin par défaut est affecté selon la méthode sélectionnée dans l'écran Spanning Tree Global Settings.

Forward Transitions. Indique le nombre de fois où le port est passé de l'état de transfert à l'état de blocage.

Remaining Hops. Indique le nombre de tronçons restant à franchir jusqu'à la destination suivante.

Onglet Multicast - IGMP Snooping

Lorsque l'option IGMP Snooping est activée globalement, tous les paquets IGMP sont transférés à l'UC. L'UC analyse les paquets entrants et détermine les éléments suivants :

- Quels ports sont à relier à quels groupes multidiffusion ?
- Quels ports disposent de routeurs multidiffusion générant des requêtes IGMP ?
- Quels protocoles de routage transfèrent des paquets et un trafic multidiffusion ?

Les ports devant être associés à un groupe multidiffusion émettent un rapport IGMP, indiquant que ce groupe multidiffusion accepte des membres. Cela entraîne la création de la base de données de filtrage multidiffusion.

Enable IGMP Snooping. Indique si l'option IGMP Snooping est activée sur le périphérique. Vous ne pouvez activer l'option IGMP Snooping que si l'option Bridge Multicast Filtering est activée.

VLAN ID. Indique l'ID de VLAN.

IGMP Status. Indique si l'option IGMP Snooping est activée sur le réseau VLAN.

Auto Learn. Indique si l'option Auto Learn est activée sur le périphérique. Si l'option Auto Learn est activée, le périphérique apprend automatiquement l'emplacement des groupes multidiffusion. Permet d'activer ou de désactiver l'option Auto Learn sur le périphérique Ethernet.

Host Timeout. Indique la durée pendant laquelle un hôte attend de recevoir un message avant qu'un dépassement de délai n'ait lieu. La valeur par défaut est de 260 secondes.

MRouter Timeout. Indique la durée pendant laquelle le routeur multidiffusion attend de recevoir un message avant qu'un dépassement de délai n'ait lieu. La valeur par défaut est de 300 secondes.

Leave Timeout. Indique la durée pendant laquelle l'hôte attend de recevoir un message en provenance d'une autre station après sa demande de sortie du groupe IGMP, avant qu'un dépassement de délai n'ait lieu. En cas de dépassement de délai, le commutateur demande au périphérique multidiffusion d'arrêter le transfert du trafic. La valeur de Leave Timeout est soit définie par l'utilisateur, soit une valeur temporaire. La valeur par défaut est de 10 secondes.

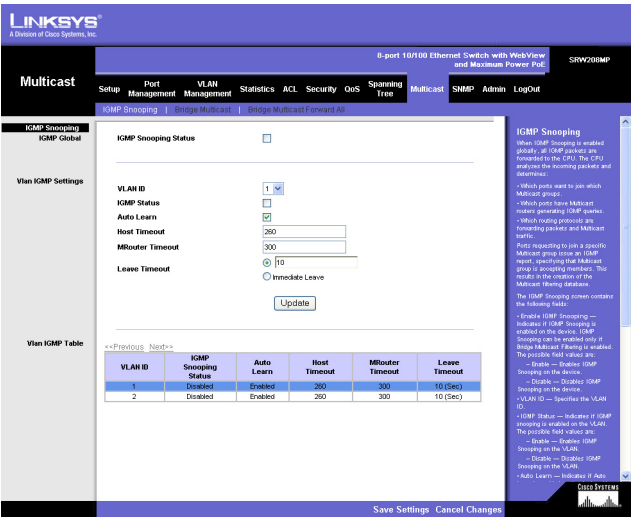


Figure 5-53 : Multicast - IGMP Snooping

Onglet Multicast - Bridge Multicast

L'écran Bridge Multicast affiche les ports et les LAG connectés au groupe de services multidiffusion dans les tables de ports et de LAG. Les tables de ports et de LAG illustrent également la façon dont les ports ou les LAG sont reliés au groupe multidiffusion. Vous pouvez ajouter des ports aux groupes existants ou aux nouveaux groupes de services multidiffusion. L'écran Bridge Multicast permet de créer de nouveaux groupes de services multidiffusion. Il permet également d'affecter des ports à un groupe spécifique d'adresses de services multidiffusion.

L'écran Bridge Multicast se divise en deux zones (Configuring Multicast et Multicast Table). Les champs sont identiques dans les deux zones.

VLAN ID. Indique un réseau VLAN à configurer en service multidiffusion.

Bridge Multicast Address. Indique l'adresse MAC/adresse IP du groupe multidiffusion.

Bridge IP Multicast. Affiche le port pouvant être ajouté à un service multidiffusion.

LAG. Affiche le LAG pouvant être ajouté à un service multidiffusion.

Les options de configuration sont les suivantes :

- **Static.** Indique que le port a été défini par l'utilisateur.
- **Dynamic.** Indique que le port est configuré dynamiquement.
- **Forbidden.** Les ports interdits ne sont pas inclus dans le groupe multidiffusion, même si l'option IGMP Snooping désignait ce port pour rejoindre un groupe multidiffusion.
- **None.** Le port n'est pas configuré pour le service multidiffusion.

Le bouton **Add to List** permet d'ajouter l'événement RMON configuré au tableau des événements, situé au bas de l'écran.

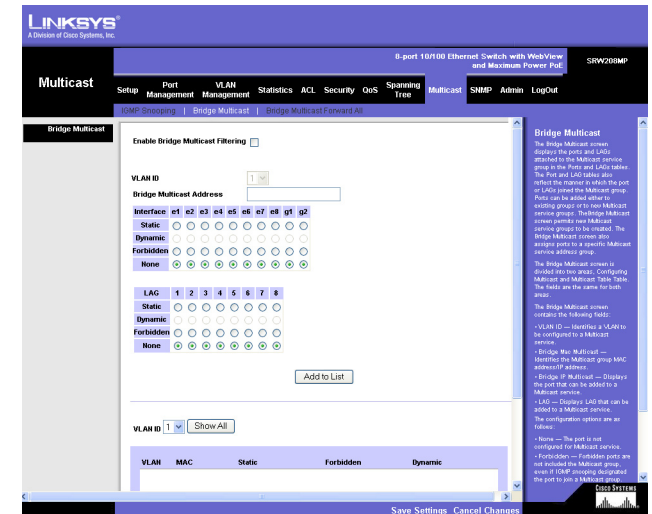


Figure 5-54 : Multicast - Bridge Multicast

Onglet Multicast - Bridge Multicast Forward All

L'écran Bridge Multicast Forward All contient des champs permettant de connecter des ports ou des LAG à un périphérique, lui-même connecté à un routeur/commutateur multidiffusion voisin. Une fois que l'option IGMP Snooping est activée, des paquets multidiffusion sont transférés vers le port ou le VLAN approprié.

L'écran Bridge Multicast Forward All contient les champs suivants :

VLAN ID. Affiche le réseau VLAN sur lequel les paramètres multidiffusion s'affichent.

Les options de configuration sont les suivantes :

- **None.** Le port n'est pas configuré pour le service multidiffusion.
- **Forbidden.** Les ports interdits ne sont pas inclus dans le groupe multidiffusion, même si l'option IGMP Snooping désignait ce port pour rejoindre un groupe multidiffusion.
- **Static.** Indique que le port a été défini par l'utilisateur.
- **Dynamic.** Indique que le port est configuré dynamiquement.

Onglet SNMP - Global Parameters

L'écran Global Parameters contient des paramètres qui permettent de définir des paramètres de notification SNMP.

Local Engine ID. Indique l'ID du moteur du périphérique local. La valeur de ce champ est une chaîne hexadécimale. Chaque octet contenu dans les chaînes de caractères hexadécimales correspond à deux chiffres hexadécimaux. Chaque octet peut être séparé par un point ou par une virgule. L'ID du moteur doit être défini avant l'activation de SNMPv3. Pour les périphériques autonomes, sélectionnez un ID de moteur par défaut composé d'un numéro d'entreprise et d'une adresse MAC par défaut. Pour les systèmes empilables, configurez l'ID du moteur, puis vérifiez qu'il est unique pour le domaine administratif concerné. Cela évite que deux périphériques d'un réseau ne portent le même ID de moteur.

Use Default. Utilise l'ID de moteur généré par le périphérique. L'ID par défaut utilise l'adresse MAC du périphérique et est défini de façon standard comme suit :

- 4 premiers octets — premier bit = 1, le reste étant le numéro d'entreprise IANA.
- Cinquième octet — 3 pour indiquer l'adresse MAC qui suit.
- 6 derniers octets — Adresse MAC du périphérique.

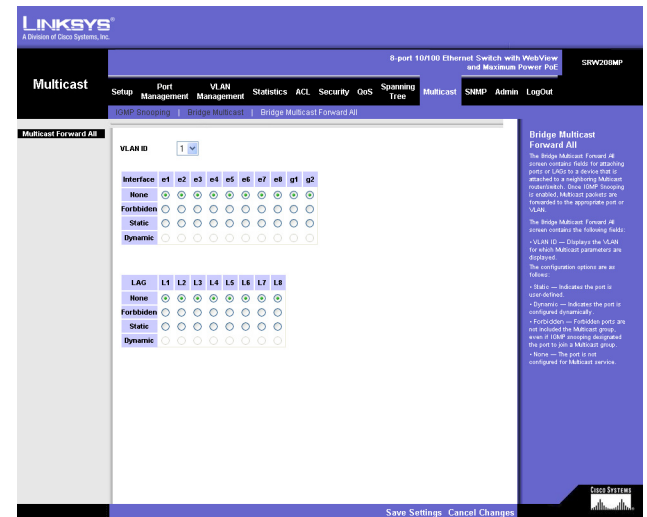


Figure 5-55 : Multicast - Bridge Multicast Forward All

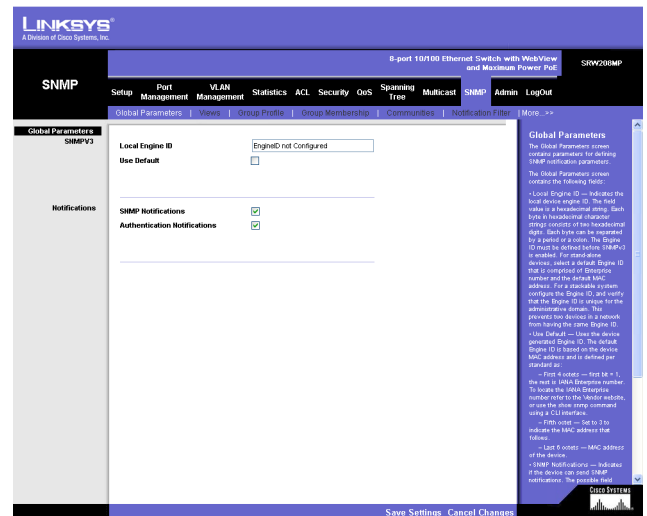


Figure 5-56 : SNMP - Global Parameters

SNMP Notifications. Indique si le périphérique peut envoyer des notifications SNMP.

Authentication Notifications. Indique si l'option de notification d'échec d'authentification SNMP est activée sur le périphérique.

Onglet SNMP - Views

Les vues SNMP permettent d'accéder ou bloquent l'accès aux fonctions de périphérique ou à certains aspects de fonctions. Par exemple, une vue peut être définie pour spécifier qu'un groupe SNMP A dispose de droits d'accès en lecture seule aux groupes multidiffusion, tandis qu'un groupe SNMP B dispose de droits d'accès en écriture aux groupes multidiffusion. L'accès aux fonctions s'effectue via le nom MIB ou l'ID d'objet MIB.

View Name. Affiche les vues définies par l'utilisateur. Les options sont les suivantes :

- **Default.** Affiche la vue SNMP par défaut des vues en lecture et lecture/écriture.
- **DefaultSuper.** Affiche la vue SNMP par défaut pour les vues de l'administrateur.

Subtree ID Tree. Indique l'OID inclus ou exclu de la vue SNMP sélectionnée. Les options de sélection de la sous-arborescence sont les suivantes :

- **Select from List.** Permet de sélectionner la sous-arborescence à partir de la liste fournie.
- **Insert.** Permet d'entrer une sous-arborescence non incluse dans le champ Select from List.

Login Type. Indique si la branche d'OID définie sera comprise dans la vue SNMP sélectionnée ou en sera exclue.

Le bouton **Add to List** permet d'ajouter la configuration de vues au tableau des vues situé au bas de l'écran.

Onglet SNMP - Group Profile

L'écran Group Profile contient des informations permettant de créer des groupes SNMP et de leur affecter des droits de contrôle d'accès. Les groupes permettent aux gestionnaires de réseaux d'affecter des droits d'accès à des fonctions spécifiques ou à des parties d'entre elles.

Group Name. Affiche le groupe défini par l'utilisateur auquel s'appliquent les règles de contrôle d'accès. La plage valide est de 30 caractères maximum.

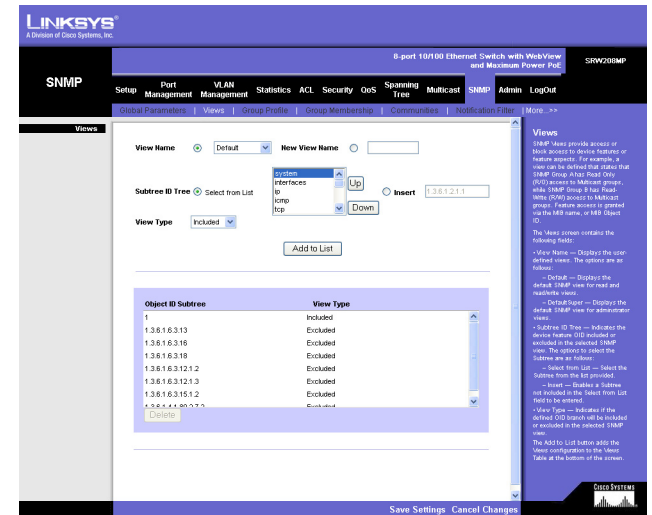


Figure 5-57 : SNMP - Views

Security Model. Définit la version SNMP associée au groupe. Les valeurs de champ possibles sont les suivantes :

- **SNMPv1.** SNMPv1 est défini pour le groupe.
- **SNMPv2.** SNMPv2 est défini pour le groupe.
- **SNMPv3.** SNMPv3 est défini pour le groupe.

Security Level. Définit le niveau de sécurité associé au groupe. Les niveaux de sécurité s'appliquent exclusivement à SNMPv3. Les valeurs de champ possibles sont les suivantes :

- **No Authentication.** Indique que les niveaux de sécurité d'authentification et de confidentialité ne sont pas affectés au groupe.
- **Authentication.** Permet d'authentifier les messages SNMP et de vérifier que l'origine des messages SNMP est authentifiée.
- **Privacy.** Effectue le cryptage des messages SNMP.

Operation. Définit les droits d'accès au groupe. Les valeurs de champ possibles sont les suivantes :

- **Read.** L'accès est limité à la lecture seule, et aucune modification ne peut être apportée à la vue SNMP affectée.
- **Write.** L'accès est limité à la lecture-écriture, et des modifications peuvent être apportées à la vue SNMP affectée.
- **Notify.** Permet d'envoyer des interceptions pour la vue SNMP affectée.

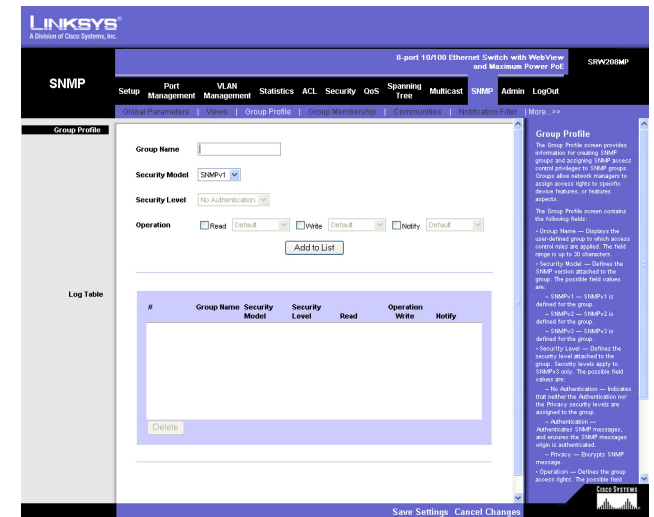


Figure 5-58 : SNMP - Group Profile

Onglet SNMP - Group Membership

L'écran Group Membership contient des informations utilisées pour l'affectation de droits de contrôle d'accès à des groupes SNMP.

User Name. Contient une liste d'utilisateurs locaux (définie par l'utilisateur).

Engine ID. Indique l'entité SNMP locale ou distante à laquelle l'utilisateur est connecté. Si vous modifiez ou supprimez l'ID d'unité SNMP, cela supprime la base de données utilisateur SNMPv3.

- **Local.** Indique que l'utilisateur est connecté à une entité SNMP locale.
- **Remote.** Indique que l'utilisateur est connecté à une entité SNMP distante. Si l'option Engine ID a été définie, les unités distantes reçoivent des messages d'information.

Group Name. Contient la liste des groupes SNMP définis par l'utilisateur. Les groupes SNMP sont définis dans la page SNMP Group Profile.

Authentication Method. Indique la méthode d'authentification utilisée. Les valeurs de champ possibles sont les suivantes :

- **None.** Indique qu'aucune méthode d'authentification n'est utilisée pour authentifier le port.
- **MD5 Password.** Indique que l'authentification de port est effectuée via l'authentification de mot de passe HMAC-MD5-96.
- **SHA Password.** Indique que l'authentification de port est effectuée via l'authentification de mot de passe HMAC-SHA-96.
- **MD5 Key.** Indique que l'authentification de port est effectuée via l'algorithme HMAC-MD5.
- **SHA Key.** Indique que l'authentification de port est effectuée via l'authentification HMAC-SHA-96.

Password. Permet de définir le mot de passe de l'utilisateur local. Les mots de passe des utilisateurs locaux peuvent contenir au maximum 159 caractères.

Authentication Key. Définit le niveau d'authentification HMAC-MD5-96 ou HMAC-SHA-96. La saisie des clés d'authentification et de confidentialité permet de définir la clé d'authentification. Si seule l'authentification est requise, 16 octets sont définis. Si la confidentialité et l'authentification sont requises, 32 octets sont définis. Chaque octet contenu dans les chaînes de caractères hexadécimaux correspond à deux chiffres hexadécimaux. Chaque octet peut être séparé par un point ou par une virgule.

Privacy Key. Définit la clé de confidentialité (LSB). Si seule l'authentification est requise, 20 octets sont définis. Si la confidentialité et l'authentification sont requises, 36 octets sont définis. Chaque octet contenu dans les chaînes de caractères hexadécimaux correspond à deux chiffres hexadécimaux. Chaque octet peut être séparé par un point ou par une virgule.

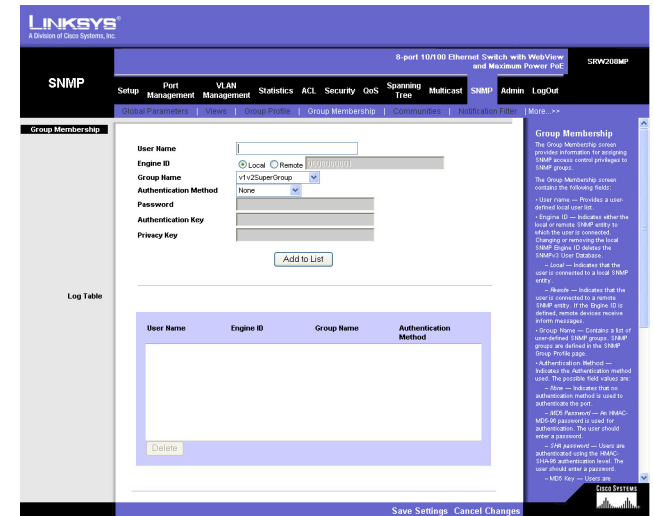


Figure 5-59 : SNMP - Group Membership

Le bouton **Add to List** permet d'ajouter la configuration de membres de groupes au tableau respectif situé au bas de l'écran.

Onglet SNMP - Communities

L'écran Communities contient trois zones (Communities, Basic Table et Advanced Table).

SNMP Management Station. Définit l'adresse IP de la station de gestion pour laquelle la communauté SNMP avancée est définie. Il existe deux options de définition :

- Définition de l'adresse IP de la station de gestion.
- **All.** Inclut toutes les adresses IP de la station de gestion.

Community String. Définit le mot de passe utilisé pour l'authentification de la station de gestion auprès du périphérique.

Basic. Active le mode SNMP Basic pour une communauté sélectionnée et contient les champs suivants :

Security Mode. Définit les droits d'accès de la communauté. Les valeurs de champ possibles sont les suivantes :

- **Read Only.** L'accès est limité à la lecture seule, et aucune modification ne peut être apportée à la communauté.
- **Read Write.** L'accès est en lecture-écriture, et des modifications peuvent être apportées à la configuration du périphérique, mais non à la communauté.
- **SNMP Admin.** L'utilisateur a accès à toutes les options de configuration du périphérique et dispose de droits de modification de la communauté.

View Name. Contient la liste des vues SNMP définies par l'utilisateur.

Advanced. Active le mode SNMP Advanced pour une communauté sélectionnée et contient les champs suivants :

Group Name. Définit des noms de groupes de communautés SNMP.

Le bouton **Add to List** permet d'ajouter la configuration de communautés au tableau correspondant situé au bas de l'écran.

Base Table

Management Station — Affiche l'adresse IP de la station de gestion pour laquelle la communauté SNMP de base est définie.

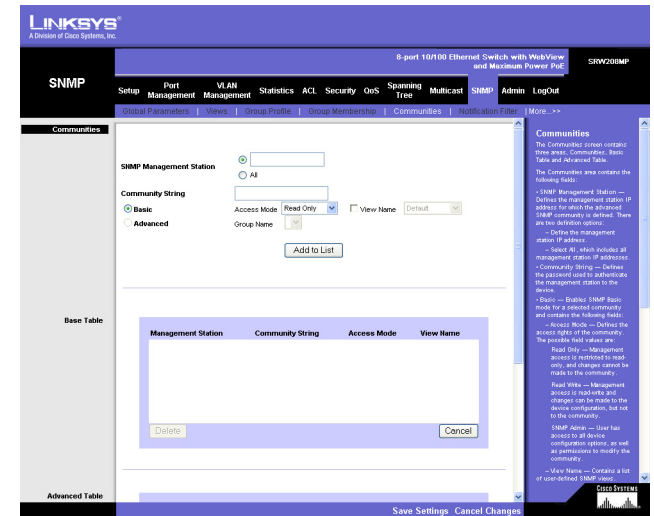


Figure 5-60 : SNMP - Communities

Community String — Affiche le mot de passe utilisé pour authentifier la station de gestion auprès du périphérique.

Access Mode — Affiche les droits d'accès de la communauté.

View Name — Affiche la vue SNMP définie par l'utilisateur.

Advanced Table

Management Station — Affiche l'adresse IP de la station de gestion pour laquelle la communauté SNMP de base est définie.

Community String — Affiche le mot de passe utilisé pour authentifier la station de gestion auprès du périphérique.

Group Name — Affiche le nom de groupe des communautés SNMP avancées.

Onglet SNMP - Notification Filter

L'écran Notification Filter permet de filtrer les interceptions sur la base des OID. Chaque OID est lié à une fonction de périphérique ou à une partie de fonction. L'écran Notification Filter permet également aux gestionnaires réseau de filtrer les notifications.

Filter Name. Contient la liste des filtres de notification définis par l'utilisateur.

New Object Identifier Subtree. Affiche l'OID pour lequel des notifications sont envoyées ou bloquées. Si un filtre est associé à un OID, des interceptions ou des messages d'information sont générés et envoyés aux destinataires. Des ID d'objet sont sélectionnés via l'option Select from List ou via l'option Object ID List. Il existe deux options de configuration :

- **Select from List.** Permet de sélectionner l'OID à partir de la liste fournie.
- **Object ID.** Permet d'entrer un OID ne figurant pas dans l'option Select from List.

Filter Type. Indique si des messages d'information ou des interceptions relatifs à l'OID sont envoyés aux destinataires.

- **Excluded.** Limite l'envoi d'interceptions ou de messages d'informations.
- **Included.** Envoie des interceptions ou des messages d'informations relatifs aux OID.

Le bouton **Add to List** permet d'ajouter la configuration de filtre de notification au tableau correspondant, situé au bas de l'écran.

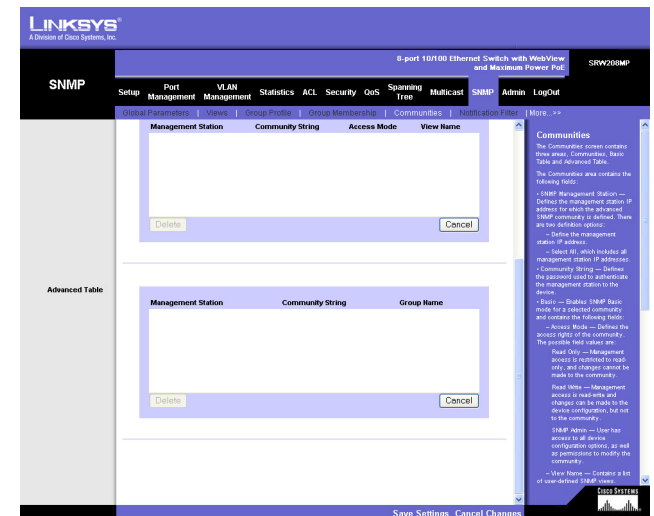


Figure 5-61 : SNMP - Notification Filter

Onglet SNMP - Notification Recipient

L'écran Notification Recipient contient des informations qui permettent de définir des filtres utilisés pour déterminer si des interceptions doivent être envoyées à des utilisateurs spécifiques, ainsi que le type d'interception à envoyer. Les filtres de notification SNMP fournissent les services suivants :

- Identification des cibles d'interceptions de gestion
- Filtrage des interceptions
- Sélection de paramètres de création d'interceptions
- Vérifications de contrôle d'accès

Recipient IP. Indique l'adresse IP de destination des interceptions.

Notification Type. Définit la notification envoyée. Les valeurs de champ possibles sont les suivantes :

- **Traps.** Indique que des interceptions sont envoyées.
- **Informs.** Indique que des messages d'informations sont envoyés.

SNMPv1,2. Active SNMPv1,2 en tant que destinataire de la notification. Vous pouvez activer SNMPv1,2 ou SNMPv3 à tout moment, mais vous ne pouvez pas les activer simultanément. Si SNMPv1,2 est activé, les champs Community String et Notification Version sont activés à des fins de configuration.

- **Community String.** Identifie la chaîne de communauté du gestionnaire d'interception.
- **Notification Version.** Détermine le type d'interception. Les valeurs de champ possibles sont les suivantes :
 - SNMP V1. Indique que des interceptions SNMP Version 1 sont envoyées.
 - SNMP V2. Indique que des interceptions SNMP Version 2 sont envoyées.

SNMPv3. Active SNMPv3 en tant que destinataire de notification. Vous pouvez activer SNMPv1,2 ou SNMPv3 à tout moment, mais vous ne pouvez pas les activer simultanément. Si SNMPv3 est activé, les champs User Name et Security Level sont activés à des fins de configuration :

User Name. Définit l'utilisateur destinataire des notifications SNMP.

Security Level. Définit la méthode utilisée pour l'authentification du paquet. Les valeurs de champ possibles sont les suivantes :



Figure 5-62 : SNMP - Notification Recipient

- **No Authentication.** Indique que le paquet n'est ni authentifié, ni chiffré.
- **Authentication.** Indique que le paquet est authentifié.
- **Privacy.** Indique que le paquet est authentifié et crypté.

UDP Port. Affiche le port UDP utilisé pour l'envoi des notifications. La valeur par défaut est de 162.

Filter Name. Indique le filtre SNMP pour lequel le filtre de notification SNMP est défini.

Timeout. Indique la durée (en secondes) pendant laquelle le périphérique attend avant de renvoyer les messages d'informations. La valeur par défaut est de 15 secondes.

Retries. Indique le nombre de nouvelles tentatives d'envoi d'une demande d'information. La valeur par défaut est de 3 secondes.

Le bouton **Add to List** permet d'ajouter la configuration de destinataire de notification au tableau correspondant situé au bas de l'écran.

Onglet Admin - User Authentication

L'écran User Authentication est utilisé pour modifier des mots de passe d'utilisateurs.

Authentication Type. Définit les méthodes d'authentification d'utilisateurs. Vous pouvez sélectionner une combinaison de toutes les méthodes d'authentification. Les valeurs de champ possibles sont les suivantes :

- **Local.** Permet d'authentifier l'utilisateur au niveau du périphérique. Le périphérique contrôle le nom et le mot de passe de l'utilisateur à des fins d'authentification.
- **RADIUS.** Permet d'authentifier l'utilisateur au niveau du serveur RADIUS.
- **TACACS+.** Permet d'authentifier l'utilisateur au niveau du serveur TACACS+.
- **None.** Permet de n'affecter aucune méthode d'authentification au profil d'authentification.

User Name. Affiche le nom de l'utilisateur.

Password. Indique le nouveau mot de passe. Le mot de passe ne s'affiche pas. Un astérisque (*) s'affiche dans le champ pour chaque caractère saisi (plage : 1 à 159 caractères).

Confirm Password. Permet de confirmer le nouveau mot de passe. Le mot de passe entré dans ce champ doit être exactement le même que celui que vous avez saisi dans le champ Password.

Le bouton **Add to List** permet d'ajouter la configuration utilisateur au tableau d'utilisateurs locaux.

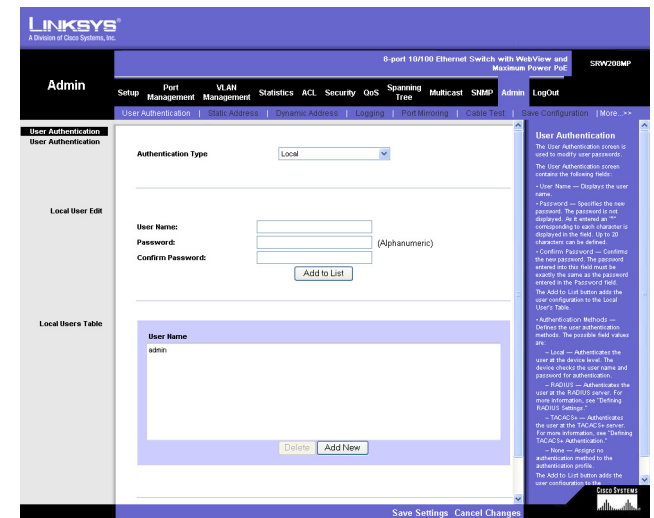


Figure 5-63 : Admin - User Authentication

Onglet Admin - Static Address

Vous pouvez affecter une adresse statique à une interface spécifique de ce commutateur. Les adresses statiques sont liées à l'interface associée et ne peuvent pas être déplacées. Lorsqu'une adresse statique est visible sur une autre interface, elle est ignorée et n'est pas enregistrée dans le tableau d'adresses.

Interface. Affiche l'interface à laquelle se réfère l'entrée :

- **Port.** Numéro de port spécifique auquel se réfèrent les paramètres de base de données de transfert.
- **LAG.** Numéro LAG spécifique auquel se réfèrent les paramètres de base de données de transfert.

MAC Address. Affiche l'adresse MAC à laquelle se réfère l'entrée.

VLAN ID. Affiche l'ID de VLAN auquel se réfère l'entrée.

VLAN Name. Affiche le nom de VLAN auquel se réfère l'entrée.

Status. Affiche le mode de création de l'entrée. Les valeurs de champ possibles sont les suivantes :

- **Permanent.** L'adresse MAC est permanente.
- **Delete on Reset.** L'adresse MAC est supprimée lorsque le périphérique est réinitialisé.
- **Delete on Timeout.** L'adresse MAC est supprimée en cas de dépassement de délai.
- **Secure.** L'adresse MAC est définie pour les ports verrouillés.

Query

Port. Indique l'interface pour laquelle la table est interrogée. Vous avez le choix entre deux types d'interfaces :

- **Port.** Numéro de port spécifique.
- **LAG.** Numéro de LAG spécifique.

MAC Address. Indique l'adresse MAC pour laquelle la table est interrogée.

VLAN ID. Indique l'ID de VLAN pour lequel la table est interrogée.

Address Table Sort Key. Indique le mode de tri de la table d'adresses MAC dynamiques. La table d'adresses peut être triée par adresse, par VLAN ou par interface.

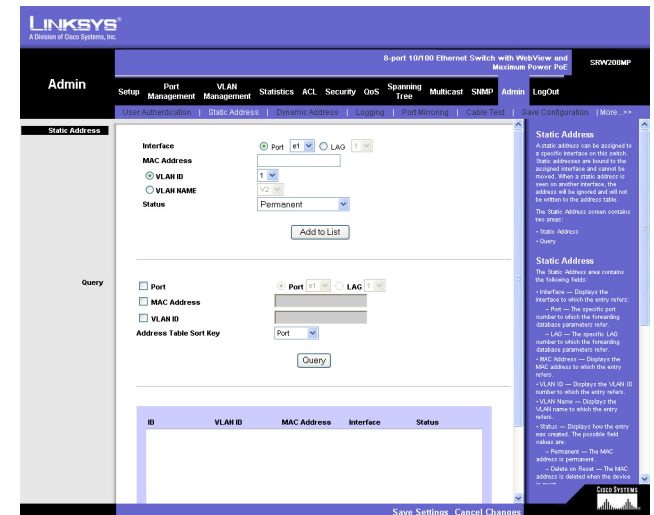


Figure 5-64 : Admin - Static Address

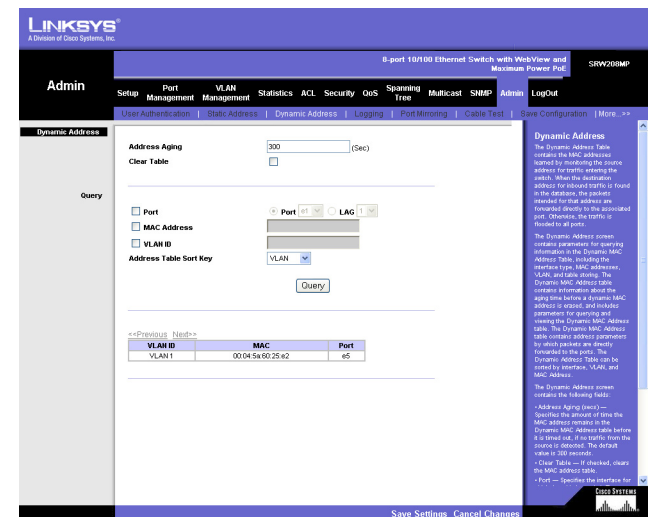


Figure 5-65 : Admin - Dynamic Address

Onglet Admin - Dynamic Address

La table d'adresses dynamiques contient les adresses MAC obtenues par la surveillance de l'adresse source pour le trafic entrant dans le commutateur. Lorsque l'adresse de destination de trafic entrant est trouvée dans la base de données, les paquets destinés à cette adresse sont transmis directement au port associé. Sinon, le trafic est acheminé vers tous les ports.

L'écran Dynamic Address contient des paramètres qui permettent de rechercher des informations dans la table des adresses MAC dynamiques (type d'interface, adresses MAC, VLAN et enregistrement de table). La table des adresses MAC dynamiques contient des informations sur le délai avant effacement d'une adresse dynamique et inclut des paramètres qui permettent d'interroger et d'afficher la table des adresses MAC dynamiques. La table des adresses MAC dynamiques contient des paramètres utilisés pour le transfert direct de paquets aux ports. Cette table peut être triée par interface, par VLAN et par adresse MAC.

Address Aging. Indique la durée (en secondes) pendant laquelle l'adresse MAC est conservée dans la table des adresses MAC dynamiques avant d'arriver à expiration, si aucun trafic en provenance de la source n'est détecté. La valeur par défaut est de 300 secondes.

Clear Table. Si cette case est cochée, la table des adresses MAC est effacée.

Query

Port. Indique l'interface pour laquelle la table est interrogée. Vous avez le choix entre deux types d'interfaces :

- **Port.** Numéro de port spécifique.
- **LAG.** Numéro de LAG spécifique.

MAC Address. Indique l'adresse MAC pour laquelle la table est interrogée.

VLAN ID. Indique l'ID de VLAN pour lequel la table est interrogée.

Address Table Sort Key. Indique le mode de tri de la table d'adresses MAC dynamiques. La table d'adresses peut être triée par adresse, par VLAN ou par interface.

Onglet Admin - Logging

Les journaux système activent l'affichage des événements de périphérique en temps réel, ainsi que leur enregistrement à des fins d'utilisation ultérieure. Les journaux système enregistrent et gèrent les événements et affichent les erreurs ou des messages d'informations.

Les messages d'événements ont un format unique, conformément au format de messages recommandé pour les rapports d'erreur SYSLOG. Par exemple, les messages Syslog et les messages de périphériques locaux disposent d'un code de gravité et incluent une abréviation permettant d'identifier l'application source à l'origine du message. Cela permet de filtrer les messages sur la base de leur urgence ou de leur pertinence. Le niveau de gravité de chaque message détermine l'ensemble d'unités de journalisation d'événements envoyé lors de chaque journalisation d'événements.

Logging. Indique si les journaux de périphériques globaux sont activés pour les mémoires cache, les fichiers et les serveurs. Par défaut, les journaux de console sont activés.

- **Emergency.** Le système ne fonctionne pas.
- **Alert.** Le système a besoin d'une intervention immédiate.
- **Critical.** L'état du système est critique.
- **Error.** Une erreur système s'est produite.
- **Warning.** Un avertissement système s'est produit.
- **Notice.** Le système fonctionne correctement, mais une notification système a été émise.
- **Informational.** Fournit des informations sur les périphériques.
- **Debug.** Fournit des informations détaillées sur le journal. Si une erreur de type Debug survient, contactez le service de support technique.

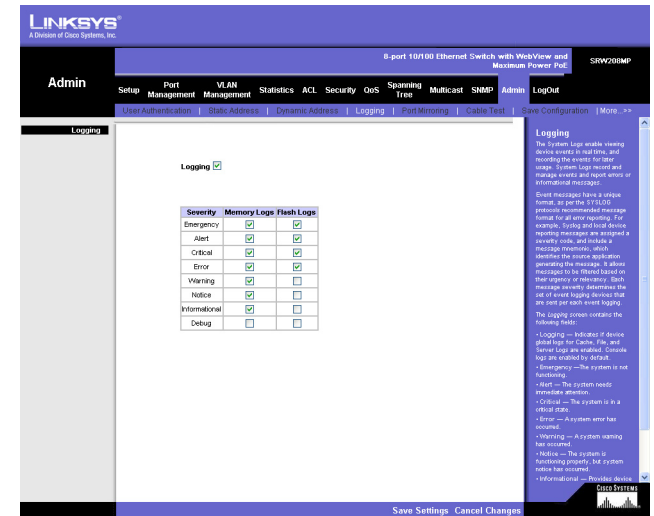


Figure 5-66 : Admin - Logging

Onglet Admin - Port Mirroring

La fonction miroir de ports permet de surveiller le trafic réseau en envoyant des copies de paquets entrants et sortants de l'un des ports vers un port chargé de la surveillance. Vous pouvez utiliser cette fonction en tant qu'outil de diagnostic et/ou à des fins de débogage. La fonction miroir de ports permet également d'effectuer le suivi des performances des commutateurs.

Les administrateurs réseau configurent la fonction miroir de ports en sélectionnant un port pour la copie de tous les paquets, ainsi que différents ports à partir desquels les paquets sont copiés.

Source Port. Définit le port utilisé pour la fonction miroir.

Type. Indique la configuration de mode de port utilisée pour la fonction miroir. Les valeurs de champ possibles sont les suivantes :

- **RxOnly.** Définit la fonction miroir de ports sur les ports récepteurs. Il s'agit de la valeur par défaut.
- **TxOnly.** Définit la fonction miroir sur les ports effectuant le transfert.

Both. Définit la fonction miroir de ports sur les ports récepteurs et émetteurs.

Target Port. Définit le port à partir duquel le trafic est mis en miroir.

Onglet Admin - Cable Test

L'écran Cable Test affiche les résultats des tests de performances réalisés sur des câbles en cuivre. La longueur maximale de câble testée est de 120 mètres. Les câbles sont testés lorsque les ports ne fonctionnent pas, sauf pour le test de longueur de câble approximative.

Port. Port auquel le câble est connecté.

Test Result. Résultat du test. OK indique que le test a été positif pour le câble. No Cable signifie qu'aucun câble n'est connecté au port. Open Cable signifie que le câble est connecté d'un seul côté. Short Cable indique qu'un court-circuit s'est produit dans le câble. Undefined indique que le test n'a pas pu être réalisé correctement.

Cable Fault Distance. Distance à partir du port sur lequel l'erreur de câble s'est produite.

Last Update. Il s'agit de la date de la dernière mise à jour du port.

Test. Cliquez sur le bouton **Test** pour exécuter le test.

Cable Length. Longueur approximative du câble. Le test de longueur de câble ne peut être réalisé que lorsque le port est actif et fonctionne à 1 Gbits/s.

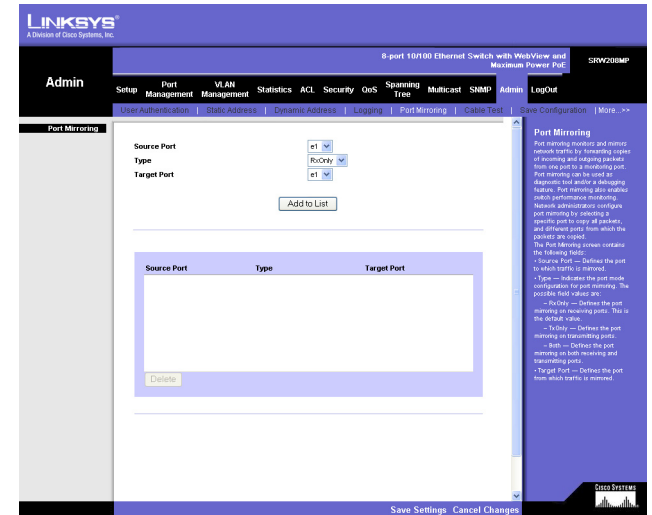


Figure 5-67 : Admin - Port Mirroring

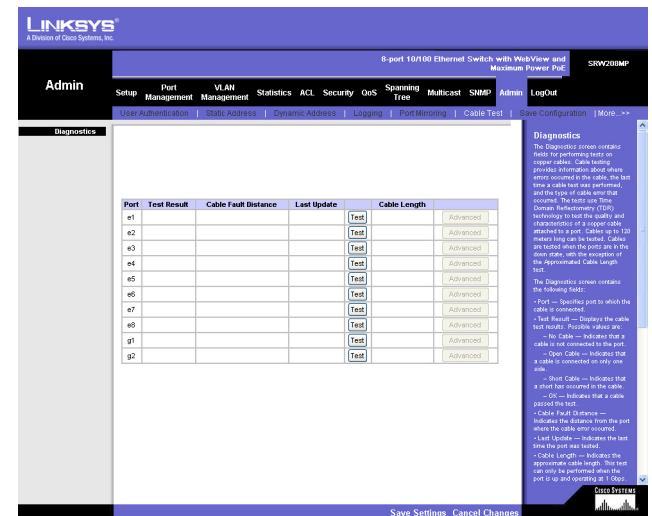


Figure 5-68 : Admin - Cable Test

Onglet Admin - Save Configuration

Via TFTP

Une fois que vous avez téléchargé un nouveau fichier image, vous devez redémarrer le périphérique. Si vous téléchargez une nouvelle image d'amorçage, veuillez procéder comme suit :

1. Téléchargez le nouveau code d'amorçage. NE RÉINITIALISEZ PAS LE PÉRIPHÉRIQUE !
2. Téléchargez la nouvelle image logicielle.
3. Réinitialisez maintenant le périphérique.

Upgrade. Sélectionnez cette option pour mettre le commutateur à niveau à partir d'un fichier situé sur un serveur TFTP.

- **TFTP Server.** Adresse IP du serveur TFTP contenant le fichier source à partir duquel la mise à niveau doit être effectuée.
- **Source File.** Indique le nom du fichier de mise à niveau sur le serveur TFTP.

Backup. Pour sauvegarder la configuration du commutateur via TFTP, entrez l'adresse du serveur TFTP.

- **TFTP Server.** Indique l'adresse IP du serveur TFTP sur lequel le fichier de configuration doit être enregistré.
- **Destination File.** Indique le nom du fichier de configuration. La valeur par défaut est StartupCfg.cfg.

Via HTTP

L'écran HTTP Firmware Upgrade est utilisé pour l'enregistrement des informations de configuration à l'aide du navigateur Web.

Upgrade. Sélectionnez cette option pour mettre le commutateur à niveau à partir d'un fichier situé sur le disque dur local.

- **Source File.** Saisissez le nom et l'emplacement du fichier, ou recherchez-le en parcourant l'arborescence de fichiers.

Backup

- **Proceed.** Le bouton Proceed est utilisé pour effectuer la sauvegarde de la configuration sur le disque dur local.

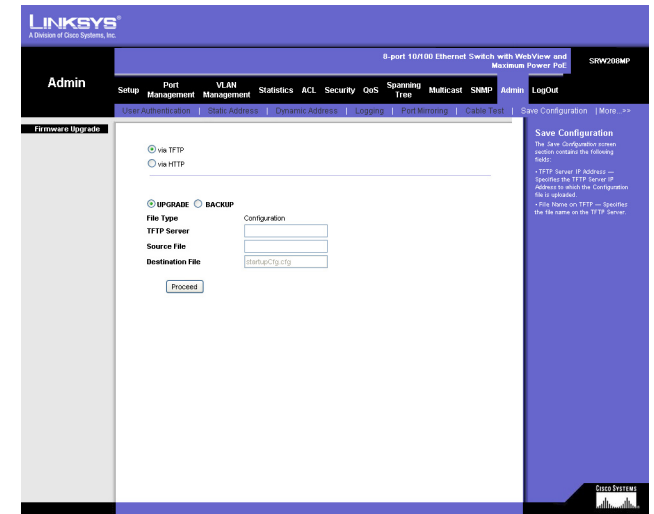


Figure 5-69 : Admin - Save Configuration



REMARQUE : lorsque vous téléchargez un fichier de configuration, vérifiez qu'il s'agit d'un fichier de configuration valide. Si vous avez modifié le fichier, assurez-vous que seules des entrées valides ont été configurées.

Onglet Admin - Firmware Upgrade

L'écran Firmware Upgrade contient les champs suivants :

via TFTP. Définit la mise à niveau via un serveur TFTP.

via HTTP. Permet d'effectuer la mise à niveau du micrologiciel à l'aide du navigateur Web.

Upgrade. Définit les fonctionnalités de l'écran en tant que mise à niveau de micrologiciel.

Backup. Définit les fonctionnalités de l'écran en tant que sauvegarde de micrologiciel.

TFTP Server IP Address. Indique l'adresse IP de serveur TFTP à partir de laquelle les fichiers sont téléchargés.

Source File Name. Indique le fichier à télécharger.

Destination File name. Indique le type de fichier de destination vers lequel le fichier est téléchargé. Les valeurs de champ possibles sont les suivantes :

- **Software Image.** Télécharge le fichier image.
- **Boot Code.** Télécharge le fichier d'initialisation.

Onglet Admin - Reboot

L'écran Reboot permet de réinitialiser le périphérique. La configuration du périphérique est automatiquement enregistrée avant le redémarrage de ce dernier.

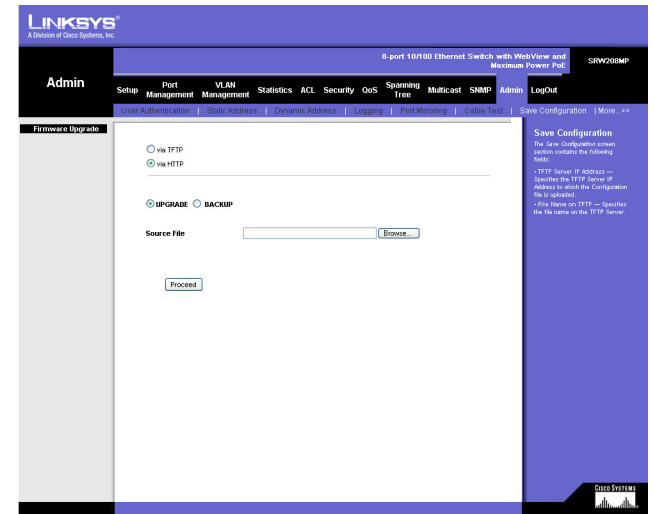


Figure 5-70 : Admin - Firmware Upgrade

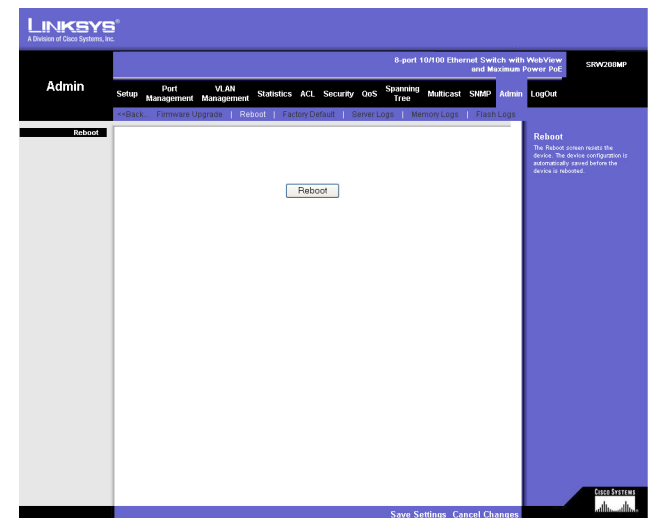


Figure 5-71 : Admin - Reboot

Onglet Admin - Factory Defaults

L'écran Factory Defaults permet aux gestionnaires réseau de restaurer les valeurs par défaut fournies avec le commutateur. Si les valeurs par défaut sont restaurées, cela efface le fichier de configuration.



REMARQUE : la restauration des valeurs par défaut efface tous les paramètres de configuration effectués. Vous pouvez sauvegarder votre configuration actuelle dans l'écran *Admin - Save Configuration*.

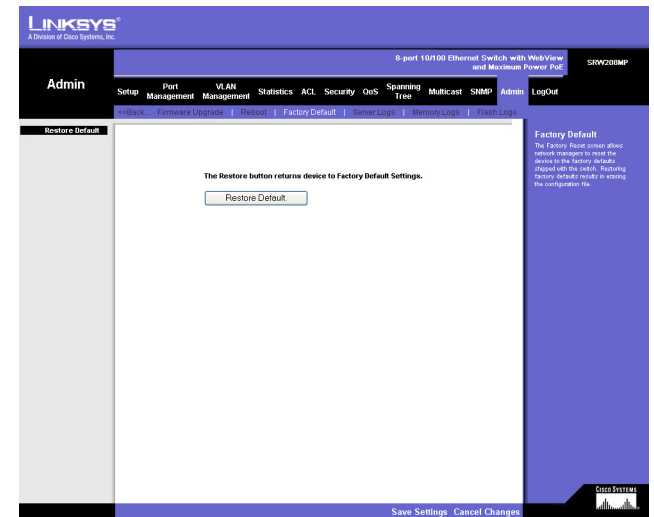


Figure 5-72 : Admin - Factory Defaults

Onglet Admin - Server Logs

L'écran Server Logs contient des informations relatives à l'affichage et à la configuration des serveurs de journalisation distants. De nouveaux serveurs de journalisation peuvent être définis, et le niveau de gravité correspondant peut être envoyé à chaque serveur.

Server. Indique le serveur auquel les journaux peuvent être envoyés.

UDP Port (1-65535). Définit le port UDP auquel les journaux serveur sont envoyés. La plage acceptée est comprise entre 1 et 65535. La valeur par défaut est 514.

Facility. Indique une application définie par l'utilisateur à partir de laquelle les journaux système sont envoyés au serveur distant. Une seule application peut être affectée à un serveur. Si une deuxième application est affectée, la première est remplacée. Toutes les applications définies pour un périphérique utilisent la même application sur un serveur. La valeur par défaut de ce champ est Local 7. Les valeurs possibles sont comprises entre Local 0 et Local 7.

Description. Fournit une description du serveur définie par l'utilisateur.

Minimum Severity. Indique le niveau de gravité minimum à partir duquel les journaux sont envoyés au serveur. Par exemple, si le niveau Notice est sélectionné, tous les journaux affichant ce niveau et les niveaux supérieurs sont envoyés au serveur distant.

Le bouton **Add to List** permet d'ajouter la configuration de journal serveur au tableau de journaux serveur, situé au bas de l'écran.



Figure 5-73 : Admin - Server Logs

Onglet Admin - Memory Logs

L'écran Memory Log contient tous les journaux système, classés par ordre chronologique, enregistrés dans la mémoire RAM (cache).

Log Index. Affiche le numéro de journal.

Log Time. Affiche l'heure à laquelle le journal a été créé.

Severity. Affiche le niveau de gravité du journal.

Description. Affiche le texte du message de journal.

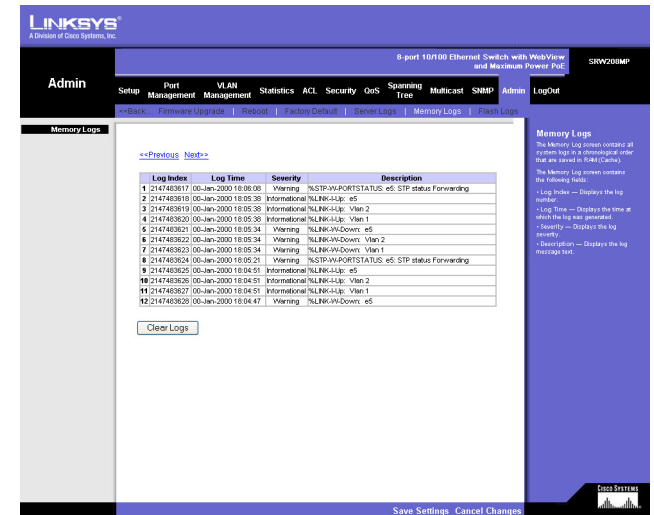


Figure 5-74 : Admin - Memory Logs

Onglet Admin - Flash Logs

L'écran Flash Log contient des informations relatives aux entrées de journaux enregistrées dans le fichier journal situé dans FLASH (heure de création du journal, niveau de gravité et description du message de journal). Le journal des messages est disponible une fois le redémarrage effectué.

Log Index. Affiche le numéro de journal.

Log Time. Affiche l'heure à laquelle le journal a été créé.

Severity. Affiche le niveau de gravité du journal.

Description. Affiche le texte du message de journal.

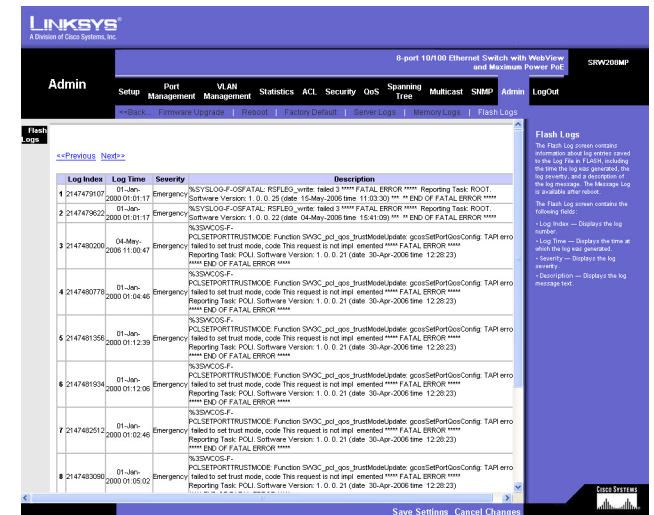


Figure 5-75 : Admin - Flash Logs

Annexe A : À propos de Gigabit Ethernet et du câblage fibre optique

Gigabit Ethernet

Gigabit Ethernet s'exécute à des vitesses de 1 Gbit/s (gigabit par seconde). Il est donc dix fois plus rapide que Fast Ethernet qui affiche un débit de 100 Mbits/s, mais s'intègre toujours de manière homogène avec du matériel Fast Ethernet (100 Mbits/s). Les utilisateurs peuvent connecter le matériel Gigabit Ethernet à l'aide soit d'un câblage par fibre optique, soit d'un câblage avec du cuivre de catégorie 5e, les fibres optiques convenant mieux aux réseaux fédérateurs. Comme la norme Gigabit s'intègre progressivement dans les réseaux existants, les applications informatiques actuelles vont bénéficier d'un temps d'accès plus rapide aux données des réseaux, au matériel et aux connexions Internet.

Câblage fibre optique

Le câblage fibre optique est réalisé à partir de plusieurs brins de verre d'une haute efficacité optique et qui sont protégés par des tubes en caoutchouc. Les fibres optiques utilisent les photons de la lumière à la place des électrons pour envoyer et recevoir des données. Bien que la fibre optique soit physiquement capable de transporter des terabits de données par seconde, le matériel de signalisation actuellement disponible sur le marché ne peut pas prendre en charge plus de quelques gigabits de données par seconde.

Les câbles en fibres optiques sont livrés avec deux types de connecteurs principaux. Le câble fibre optique le plus couramment utilisé est le câble fibre optique multimode (MMF), avec une âme de fibre optique de 62,5. Le câblage en fibre optique monomode est sensiblement plus efficace que le multimode mais il est beaucoup plus cher, en raison de son âme optique plus petite qui aide à retenir l'intensité des signaux lumineux qui passent. Une connexion par fibre optique nécessite toujours deux câbles à fibres optiques : l'un transmet les données et l'autre les reçoit.

Chaque câble en fibre optique est muni d'un connecteur qui se loge dans un port pour fibre optique sur un adaptateur réseau, un concentrateur ou un commutateur. Aux États-Unis, la plupart des câbles utilisent un connecteur SC carré qui se glisse et se verrouille en position lorsqu'il est branché dans un port ou connecté à un autre câble. En Europe, le connecteur ST rond est plus courant.

Vous devez utiliser les modules Linksys MGBT1, MGBSX1 ou MGBLH1 mini-GBIC avec les commutateurs gigabit Linksys. Les modules MGBSX1 et MGBLH1 nécessitent un câblage fibre optique avec des connecteurs LC, et le module MGBT1 nécessite un câble Ethernet catégorie 5e avec un connecteur RJ-45.

Annexe B : Aide de Windows

Presque tous les produits réseau requièrent Microsoft Windows. Windows est le système d'exploitation le plus répandu au monde. Il propose un grand nombre de fonctionnalités qui facilitent la mise en réseau. Vous pouvez accéder à ces fonctionnalités à partir de l'aide de Windows. Elles sont décrites dans la présente annexe.

TCP/IP

Pour qu'un ordinateur puisse communiquer au sein d'un réseau, vous devez au préalable activer le protocole TCP/IP. TCP/IP désigne un ensemble d'instructions (ou protocole) que tous les ordinateurs suivent pour communiquer sur un réseau. Il s'applique aussi dans le cadre des réseaux sans fil. Vos ordinateurs ne pourront pas exploiter les capacités de votre réseau sans fil si le protocole TCP/IP n'est pas activé. L'aide de Microsoft Windows fournit des instructions exhaustives sur l'activation du protocole TCP/IP.

Ressources partagées

Si vous souhaitez partager des imprimantes, un dossier ou des fichiers sur votre réseau, l'aide de Windows offre également des instructions complètes sur l'utilisation des ressources partagées.

Voisinage réseau/Favoris réseau

En fonction de la version de Windows que vous utilisez, d'autres ordinateurs de votre réseau peuvent apparaître dans le Voisinage réseau ou dans les Favoris réseau. Là encore, l'aide de Windows fournit des instructions expliquant comment ajouter des ordinateurs à votre réseau.

Annexe C : Téléchargement à l'aide de Xmodem

Procédures du menu Startup

Il est possible d'entrer dans le menu Startup lors de l'amorçage du périphérique. Une fenêtre s'affiche pendant deux secondes permettant d'accéder au menu Startup immédiatement après le test POST. Il est possible d'accéder au menu directement à partir d'un terminal connecté sur le port de la console. Les procédures du menu Startup peuvent être effectuées en utilisant le terminal ASCII ou l'HyperTerminal Windows.

La procédure de téléchargement du logiciel est effectuée lorsqu'une nouvelle version doit être téléchargée pour remplacer des fichiers corrompus, pour mettre à jour ou mettre à niveau le logiciel système. Pour télécharger le logiciel à partir du menu Startup :

Pour entrer dans le menu Startup :

1. Mettez votre ordinateur et le commutateur sous tension.
2. Connectez le câble simulateur de modem nul du port COM de votre ordinateur au port Console sur le commutateur.
3. Mettez votre ordinateur sous tension et lancez HyperTerminal, suivez les instructions du **Chapitre 4 : Utilisation de l'interface de la console pour la configuration** pour configurer HyperTerminal pour connecter le commutateur.
4. Mettez le commutateur sous tension et attendez le message d'autoamorçage :

Autoboot in 2 seconds - press RETURN or Esc. to abort and enter prom.

5. Lorsque le message d'auto amorçage apparaît, appuyez sur la touche **Entrée** pour accéder au menu Startup.



REMARQUE : si aucune sélection n'est effectuée dans les 35 secondes (valeur par défaut), le temps d'attente est alors dépassé et vous devrez débrancher l'alimentation électrique pour redémarrer le processus.

6. Sélectionnez [1] Download Software et un message va apparaître, *Downloading code using XMODEM* avec des caractères s'affichant à l'écran. Si vous n'effectuez pas les étapes sur la page suivante pour localiser le fichier à télécharger dans un certain laps de temps, le périphérique se réinitialisera.
7. Sélectionnez **Send file** dans le menu déroulant *Transfer*.

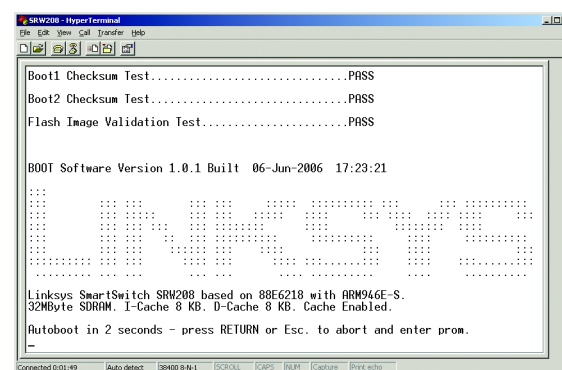


Figure C-1 : Messages d'autoamorçage

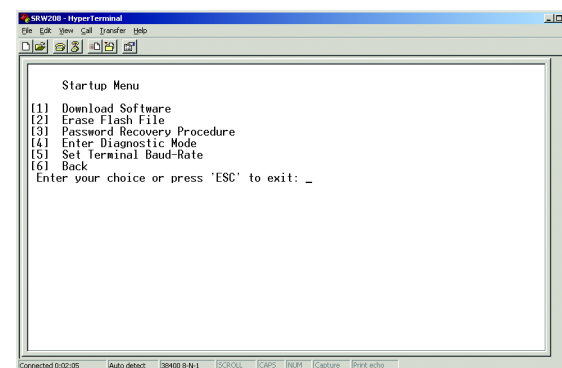


Figure C-2 : Startup Menu

8. Dans le champ *Filename* : saisissez le chemin du fichier à télécharger ou cliquez sur **Browse** pour localiser le fichier.

Seuls les fichiers valides, avec une extension *.ros ou *.rft, qui ont été fournis par Linksys, peuvent être téléchargés. Le téléchargement de fichiers non valides se traduira par un comportement imprévisible.

Assurez-vous que le protocole Xmodem est sélectionné dans le champ *Protocol* :

9. Appuyez sur **Send** et le logiciel est téléchargé.

Une fois que le logiciel a été téléchargé, le périphérique redémarrera automatiquement.

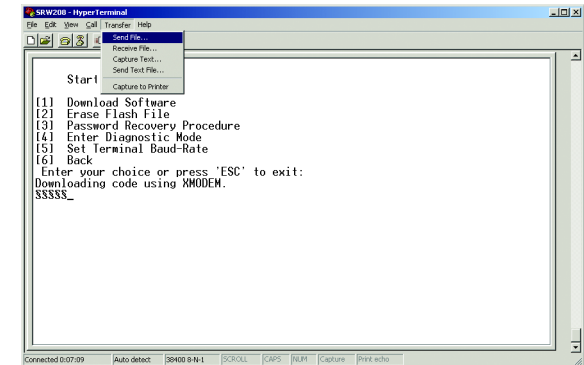


Figure C-3 : Envoyer le fichier

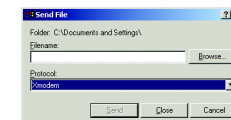


Figure C-4 : Téléchargement

Annexe D : Glossaire

Ce glossaire contient des termes de base du domaine des réseaux que vous pourrez rencontrer en utilisant ce produit. Pour des termes plus évolués, consultez le glossaire Linksys complet à l'adresse suivante : <http://www.linksys.com/glossary>.

ACE : filtres des listes de contrôle d'accès (ACL) qui déterminent quel trafic réseau est redirigé. Un ACE est basé sur les critères suivants :

- Protocole
- ID de Protocole
- Port source
- Port de destination
- Masque de caractères génériques
- Adresse IP source
- Adresse IP de destination

ACL (Access Control List) : les listes de contrôle d'accès sont utilisées pour autoriser, refuser ou limiter l'accès aux périphériques, aux fonctions ou aux applications.

Adresse IP : adresse utilisée pour l'identification d'un ordinateur ou d'un périphérique sur un réseau.

Adresse IP dynamique : adresse IP attribuée provisoirement par un serveur DHCP.

Adresse IP statique : adresse fixe attribuée à un ordinateur ou périphérique connecté à un réseau.

Adresse MAC (Media Access Control) : adresse unique qu'un fabricant attribue à chaque périphérique réseau.

Agrégation de liens : réunion de plusieurs liens de communication. Optimise l'utilisation des ports en reliant ensemble un groupe de port pour former un seul tronçon (groupes agrégés).

Amorçage : démarrer un périphérique et faire en sorte qu'il commence à exécuter des instructions.

Attributions de bande passante : indique la quantité de bande passante attribuée à une application, un utilisateur et/ou une interface spécifiques.

Avalanche de messages diffusés : quantité excessive de messages diffusés simultanément transmis sur un réseau par un seul port. Les réponses des messages transmis sont accumulées sur le réseau, ce qui surcharge les ressources réseau ou provoque un arrêt du réseau.

Back Pressure : mécanisme utilisé avec le mode semi-duplex qui autorise un port à ne pas recevoir un message.

Bande passante : capacité de transmission d'un périphérique ou d'un réseau donné.

Baud : indique le nombre d'éléments de signalisation transmis chaque seconde.

Bit : chiffre binaire.

Cartes de classe : aspect du système de qualité de service qui se compose d'un ACL IP et/ou d'un ACL MAC. Les cartes de classes sont configurées pour correspondre à des critères de paquets, et sont mises en correspondance avec les paquets dans un mode d'ajustement initial.

CBS (Committed Burst Size) : indique le nombre maximal de bits de données transmis dans un intervalle de temps spécifique.

CIR (Committed Information Rate) : le taux de données est moyenné au-dessus d'un incrément de temps minimal.

Communautés : indique un groupe d'utilisateurs qui détiennent les mêmes droits d'accès au système.

Commutateur : filtre et transfère les paquets entre des segments de réseau local. Les commutateurs prennent en charge tout type de protocole de paquets.

Contrôle d'activité : détermine si les niveaux de trafic se trouvent au sein d'un profil spécifié. Le contrôle d'activité gère le taux de trafic maximal utilisé pour envoyer ou recevoir des paquets sur une interface.

Contrôle de flux : permet à des périphériques de vitesse plus faible de communiquer avec des périphériques à vitesse plus élevée. Cela est rendu possible par le fait que le périphérique à la vitesse la plus élevée s'abstient d'envoyer les paquets.

CoS (Class of Service) : système de priorité 802.1p. CoS fournit une méthode de balisage des paquets avec des informations relatives à la priorité. Une valeur CoS comprise entre 0 et 7 est ajoutée à l'en-tête de la couche II des paquets (zéro représentant la priorité la plus faible et sept la plus élevée).

Cryptage : codage des données transmises sur un réseau.

DDNS (Dynamic Domain Name System) : autorise l'hébergement d'un site Web, d'un serveur FTP ou d'un serveur de messagerie avec un nom de domaine fixe (par exemple, www.xyz.com) et une adresse IP dynamique.

Débit : quantité de données déplacées avec succès d'un nœud à un autre dans un délai donné.

Débit TX : débit de transmission.

DHCP (Dynamic Host Configuration Protocol) : protocole réseau permettant aux administrateurs d'attribuer des adresses IP temporaires aux ordinateurs du réseau en « allouant » une adresse IP à un utilisateur pour une période limitée, au lieu d'attribuer des adresses IP permanentes.

DHCP Clients : hôte Internet utilisant DHCP pour obtenir des paramètres de configuration, tels qu'une adresse réseau.

DNS (Domain Name Server) : adresse IP du serveur de votre fournisseur d'accès Internet (FAI). Le système DNS permet de convertir des noms de sites Web en adresses IP.

Domaine : nom spécifique d'un réseau d'ordinateurs.

Domaine de diffusion : ensembles de périphériques qui reçoivent les trames de diffusion en provenance de tout périphérique au sein d'un ensemble désigné. Les routeurs associent les domaines de diffusion, car ils ne transfèrent pas les trames de diffusion.

DSCP (DiffServe Code Point) : fournit une méthode de balisage des paquets IP avec des informations relatives à la priorité QoS.

DSL (Digital Subscriber Line) : connexion haut débit permanente par le biais des lignes téléphoniques standard.

EIGRP (Enhanced Interior Gateway Routing Protocol) : fournit une convergence rapide, la prise en charge d'un masque de sous-réseau de longueur variable et la prise en charge de protocoles de couches de réseau multiples.

Ethernet : protocole réseau IEEE qui spécifie le mode de placement et d'extraction des données via un support de transmission courant.

FAI (Fournisseur d'Accès Internet) : société proposant un service d'accès à Internet.

FTP (File Transfer Protocol) : protocole utilisé pour la transmission de fichiers sur un réseau TCP/IP.

Full Duplex : aptitude d'un périphérique réseau à recevoir et transmettre simultanément des données.

GARP (General Attributes Registration Protocol) : enregistre les stations clientes dans un domaine de multidiffusion.

GBIC (GigaBit Interface Converter) : module matériel utilisé pour rattacher des périphériques réseau à des systèmes de transmission basés sur fibre optique. GBIC convertit les signaux électriques en signaux optiques et vice versa.

GVRP (GARP VLAN Registration Protocol) : enregistre les stations clientes dans les réseaux VLAN.

HTTP (HyperText Transport Protocol) : protocole de communication utilisé pour la connexion à des serveurs sur Internet.

HTTPS (HyperText Transport Protocol Secure) : extension du protocole HTTP standard qui fournit une confidentialité en cryptant le trafic à partir du site Web. Par défaut, ce protocole utilise le port TCP 443.

ICMP (Internet Control Message Protocol) : permet à la passerelle ou à l'hôte de destination de communiquer avec l'hôte source. Par exemple, pour signaler une erreur de traitement.

IGMP (Internet Group Management Protocol) : permet aux hôtes d'informer leur commutateur ou leur routeur local qu'ils souhaitent recevoir des transmissions affectées à un groupe de multidiffusion spécifique.

IP (Internet Protocol) : protocole utilisé pour transmettre des données sur un réseau.

IPCONFIG : utilitaire des systèmes Windows 2000 et XP qui affiche l'adresse IP d'un périphérique réseau spécifique.

IPSec (Internet Protocol Security) : protocole VPN employé pour la mise en place d'un échange sécurisé des paquets au niveau de la couche IP.

Jumbo Frames (trames étendues) : autorisent le transport de données identiques dans un nombre réduit de trames. Elles permettent de réduire la surcharge système, diminuer le temps de traitement et garantir une réduction des interruptions.

LAG (Link Aggregated Group) : regroupe les ports ou les réseaux VLAN en un seul port ou VLAN virtuel.

LAN : ordinateurs ou périphériques mis en réseau qui constituent votre réseau local.

Masque : filtre qui inclut ou exclut certaines valeurs par exemple des parties d'une adresse IP.

Masque de caractères génériques : indique quels bits de l'adresse IP sont utilisés, et quels bits sont ignorés. Un masque de caractères génériques 255.255.255.255 indique qu'aucun bit n'est important. Le masque de caractères génériques 0.0.0.0 indique en revanche que tous les bits sont importants.

Par exemple, si l'adresse IP de destination est 149.36.184.198 et que le masque de caractères génériques est 255.36.184.00, les deux premiers bits de l'adresse IP sont utilisés, alors que les deux derniers bits sont ignorés.

Masque de sous-réseau : code d'adresse qui détermine la taille du réseau.

Mbits/s (Mégabits par seconde) : un million de bits par seconde ; unité de mesure de transmission de données.

MD5 (Message Digest 5) : algorithme qui produit un hachage 128 bits. MD5 est une variante de l'algorithme MD4, et accroît la sécurité MD4. MD5 vérifie l'intégrité de la communication et authentifie l'origine de la communication.

MDI (Media Dependent Interface) : câble utilisé pour les stations de destination.

MDIX (Media Dependent Interface with Crossover) : câble utilisé pour les concentrateurs et les commutateurs.

MIB (Management Information Base) : les MIB contiennent des informations décrivant des aspects spécifiques des composants du réseau.

Micrologiciel : code de programmation qui exécute un périphérique réseau..

Miroir de ports : surveille et effectue des duplications du trafic réseau en transmettant des copies des paquets entrants et sortants en provenance d'un port vers un port de surveillance.

Mise à niveau : acte de remplacer un logiciel ou micrologiciel existant par une nouvelle version.

Mode au mieux : indique que le trafic est affecté à la file d'attente de plus faible priorité et que la livraison du paquet n'est pas garantie.

Mode d'accès : indique la méthode par laquelle l'accès utilisateur est autorisé au système.

Modem câble : périphérique qui établit une connexion Internet par le biais d'un réseau de télévision câblé.

Multidiffusion : transmet des copies d'un paquet unique vers plusieurs ports.

Navigateur : programme d'application qui permet de rechercher et d'interagir avec toutes les informations présentes sur le World Wide Web.

Négociation automatique : autorise les ports Ethernet 10/100 Mbits/s ou 10/100/1 000 Mbits/s à établir automatiquement de manière optimale le mode duplex, le contrôle de flux et la vitesse.

NMS (Network Management System) : interface qui fournit une méthode de gestion d'un système.

Octet : unité de données généralement équivalente à huit bits.

OID (Object Identifier) : utilisé par le protocole SNMP pour identifier les objets gérés. Dans le paradigme de gestion de réseau gestionnaire/agent SNMP, chaque objet géré doit posséder un OID pour pouvoir l'identifier.

Paquet : unité de données transmise sur un réseau.

Passerelle : périphérique permettant de relier entre eux des réseaux dotés de protocoles de communication incompatibles.

Passerelle par défaut : périphérique utilisé pour transférer un trafic de données Internet depuis votre réseau local.

Ping (Packet INternet Groper) : utilitaire Internet utilisé pour déterminer si une adresse IP particulière est en ligne.

Point d'accès : périphérique permettant aux ordinateurs et aux autres périphériques sans fil de communiquer avec un réseau câblé. Également utilisé pour étendre la portée d'un réseau sans fil.

Pont : périphérique qui relie deux réseaux. Les ponts sont spécifiques au matériel, ils sont cependant indépendants du protocole. Les ponts fonctionnent au niveau de la couche 1 et de la couche 2.

Port : point de connexion sur un ordinateur ou un périphérique réseau utilisé pour le branchement à des câbles ou adaptateurs.

Ports mixtes : port logique unique doté de deux connexions physiques, incluant une connexion RJ-45 et une connexion SFP.

Power over Ethernet (PoE) : technologie permettant à un câble réseau Ethernet d'acheminer des données et l'alimentation.

Profils d'accès : permet aux gestionnaires réseau de définir des profils et des règles pour l'accès aux périphériques. L'accès aux fonctions de gestion peut être limité à des groupes d'utilisateurs, qui sont définis par les critères suivants :

- Interfaces Ingress.
- Adresse IP source/ou sous-réseaux IP sources.

QoS (Quality of Service) : fournit des stratégies qui contiennent des jeux de filtres (règles). QoS permet aux gestionnaires de réseaux de décider comment et quel trafic réseau est transféré en fonction des priorités, des types d'applications et des adresses de source et de destination.

RADIUS (Remote Authentication Dial-In User Service) : protocole utilisant un serveur d'authentification pour contrôler l'accès au réseau.

Rafale : transmission d'un paquet à une vitesse supérieure aux taux normaux. Les rafales sont limitées dans le temps et ne se produisent que dans des conditions spécifiques.

Réseau : groupe d'ordinateurs ou de périphériques reliés entre eux dans le but de partager et de stocker des données et/ou de permettre la transmission de données entre des utilisateurs.

RJ-45 (Registered Jack-45) : connecteur Ethernet pouvant accueillir jusqu'à huit broches.

RMON (Remote Monitoring) : fournit des informations réseau à recueillir à partir d'un seul poste de travail.

Routeur : périphérique réseau qui relie entre eux plusieurs ordinateurs.

RSTP (Rapid Spanning Tree Protocol) : détecte et utilise les topologies réseau qui permettent une convergence plus rapide de l'algorithme « spanning tree », sans créer de boucles de transfert.

Semi-duplex : transmission de données à double sens sur une ligne unique, mais dans un seul sens à la fois.

Serveur : tout ordinateur dont le rôle sur un réseau est de fournir aux utilisateurs un accès à des fichiers, des imprimantes, des outils de communication et d'autres services.

Serveur DHCP : hôte Internet qui retourne les paramètres de configuration vers les clients DHCP.

SMTP (Simple Mail Transfer Protocol) : protocole de messagerie standard utilisé sur Internet.

SNMP (Simple Network Management Protocol) : protocole très répandu de contrôle et d'administration de réseau.

Sous-réseau (Sub-network) : les sous-réseaux sont des parties d'un réseau qui partagent un composant d'adresse commune. Dans les réseaux TCP/IP, les périphériques qui partagent un préfixe font partie du même sous-réseau. Par exemple, tous les périphériques possédant le préfixe 157.100.100.100 font partie du même sous-réseau.

SSH : programme Secure Shell. Utilitaire qui utilise une authentification robuste et des communications sécurisées pour se connecter à un autre ordinateur sur un réseau.

SSL (Secure Socket Layer) : technologie de cryptage pour Internet utilisée pour fournir des transactions sécurisées, telles que la transmission de numéros de carte de crédit pour le commerce électronique.

STP (Spanning Tree Protocol) : évite la formation de boucles dans le trafic réseau. Le protocole Spanning Tree Protocol (STP) fournit une topographie arborescente pour toute disposition de ponts. STP fournit un chemin unique entre les stations de destination sur un réseau, en éliminant les boucles.

TACACS+ (Terminal Access Controller Access Control System Plus) : dernière version du système de contrôle d'accès du contrôleur d'accès terminal (TACACS) mis au point par CISCO. Fournit une assistance supplémentaire pour l'authentification, l'autorisation et la gestion des comptes.

Taille de la rafale : indique la taille de la rafale transmise à une vitesse supérieure au taux normal.

TCP (Transmission Control Protocol) : protocole réseau de transmission de données exigeant la validation de la personne à qui elles sont destinées.

TCP/IP (Transmission Control Protocol/Internet Protocol) : désigne un ensemble d'instructions (ou protocole) que tous les ordinateurs suivent pour communiquer sur un réseau.

Téléchargement (envoi) : transmission d'un fichier sur un réseau.

Téléchargement (réception) : réception d'un fichier transmis sur un réseau.

Telnet : commande utilisateur et protocole TCP/IP utilisés pour l'accès à des ordinateurs distants.

TFTP (Trivial File Transfer Protocol) : version du protocole FTP TCP/IP n'offrant aucune fonction de répertoire ou de mot de passe.

UDP (User Data Protocol) : protocole de communication qui transmet les paquets mais ne garantit pas leur livraison.

URL (Uniform Resource Locator) : adresse d'un fichier situé sur Internet.

VLAN (Virtual Local Area Networks) : sous-groupes logiques qui constituent un réseau local (LAN). Il s'agit d'une opération logicielle, bien plus qu'une solution matérielle.

WAN (Wide Area Network) : réseaux qui couvrent une vaste zone géographique.

Annexe E : Spécifications

SRW208

Ports	8 connecteurs RJ-45 pour 10BASE-T et 100BASE-TX Port Console Auto MDI/MDI-X Négociation automatique/Paramétrage manuel
Type de câblage	UTP CAT 5 ou qualité supérieure pour 10BASE-T/100BASE-TX
DEL	10/100 Link/Act, Speed, System

Performances

Capacité de commutation	1,6 Go sans blocage
Taux de transfert	Performances de vitesse câblée de 1,19 Mpps

Couche 2

Taille de table MAC	8 Ko
Nombre de réseaux VLAN	256 réseaux VLAN actifs (plage de 4096)
Réseau VLAN	Réseaux VLAN basés sur les ports et le marquage 802.1Q Management VLAN
Blocage HOL	Prévention du blocage de tête de ligne

Gestion

Interface utilisateur Web	IU Web intégrée pour une configuration basée sur navigateur simplifiée (HTTP/HTTPS)
SNMP	SNMP version v1, v2c, v3 avec prise en charge des interceptions.
SNMP MIB	RFC1213 MIB-2, RFC2863 Interface MIB, RFC2665 Ether-like MIB, RFC1493 pont MIB, RFC2674 pont étendu MIB (pont P, pont Q), RFC2819 RMON MIB (groupes 1, 2, 3, 9 uniquement), RFC2737 entité MIB, RFC 2618 client RADIUS MIB interceptions RFC 1215
RMON	L'agent logiciel de surveillance à distance intégré (RMON) prend en charge quatre groupes RMON (historique, statistiques, alarmes et événements) pour une gestion du trafic, une surveillance et une analyse améliorées.
Mise à niveau du micro logiciel	Mise à niveau par le navigateur Web (HTTP) et TFTP
Miroir de port RMON	Le trafic sur un port peut être dupliqué vers un autre port en vue d'une analyse avec un analyseur de réseau ou avec la sonde
Gestion d'autres éléments	Traceroute Couche d'échange sécurisé (SSL) Secure Shell (SSH) RADIUS miroir de ports Mise à niveau TFTP Sécurité SSL pour IU Web Serveur DHCP BootP SNTP Mise à niveau Xmodem Cable Diagnostics PING Client Telnet (support sécurisé SSH)

Sécurité

IEEE 802.1x 802.1x - Authentification RADIUS. Cryptage MD5

Contrôle d'accès ACL - Limite de seuil ou de taux basée sur :
 Source et destination basées sur l'adresse MAC
 Adresse IP source et de destination
 Protocole
 TOS/DSCP
 Port
 VLAN
 Ethertype

Disponibilité

Agrégation de liens Agrégation de liens conformément à la norme IEEE 802.3ad LACP
 Jusqu'à 8 ports dans 8 groupes au maximum

Contrôle d'avalanche Diffusion, multidiffusion et diffusion individuelle inconnue

Spanning Tree Spanning Tree IEEE 802.1D, Rapid Spanning Tree IEEE 802.1w, Multiple Spanning Tree IEEE 802.1s

IGMP Snooping IGMP Snooping (v1/v2) fournit pour un client rapide des réunions et des départ de flux de multidiffusion et limite le trafic vidéo gourmand en bande passante uniquement vers les demandeurs. Prend en charge 256 groupes de multidiffusion.

QoS (qualité de service)

Niveaux de priorité 4 files d'attente matérielles

Répartition Formation de files d'attentes par priorité et pondération WRR

Classe de service basée sur les ports
 Réseau VLAN 802.1p basé sur la priorité
 IPv4/v6 IP basé sur la priorité/TOS/DSCP

	TCP/UDP basé sur les ports Diffserv Classification et marquage des ACL
Limitation du taux	Contrôle de l'entrée Contrôle du taux de sortie
Normes	802.3 Ethernet 10BASE-T, 802.3u Fast Ethernet 100BASE-TX, contrôle de flux 802.3ab, 802.3x, 802.3 ad LACP, 802.1D STP, 802.1Q/p VLAN, 802.1w Rapid STP, 802.1s Multiple STP, 802.1x authentification d'accès aux ports

Environnement

Dimensions	279 mm x 44 mm x 170 mm
Poids unitaire	1 kg
Alimentation	Adaptateur externe CA
Certifications	FCC Part15 Classe A, CE Classe A, UL, cUL, marque CE, CB
Température de fonctionnement	0 à 40 °C
Température de stockage	-20 à 70 °C
Humidité en fonctionnement	10 à 90 %, non condensée
Humidité de stockage	10 à 95 %, non condensée

SRW208G

Ports	8 connecteurs RJ-45 pour 10BASE-T et 100BASE-TX, 1 connecteur RJ-45 pour 10BASE-T/100BASE-TX/1000BASE-T, et 1 port miniGBIC/SFP Port Console Auto MDI/MDI-X Négociation automatique/Paramétrage manuel
-------	---

Type de câblage	UTP CAT 5 ou qualité supérieure pour 10BASE-T/100BASE-TX, UTP CAT 5e ou qualité supérieure pour 1000BASE-T
-----------------	--

DEL	10/100 Link/Act, Giga Link/Act, Speed, miniGBIC Link/Act, Speed, System
-----	---

Performances

Capacité de commutation	5,6 Go sans blocage
-------------------------	---------------------

Taux de transfert	Performances de vitesse câblée de 4,17 Mpps
-------------------	---

Couche 2

Taille de table MAC	8 Ko
---------------------	------

Nombre de réseaux VLAN	256 réseaux VLAN actifs (plage de 4096)
------------------------	---

Réseau VLAN	Réseaux VLAN basés sur les ports et le marquage 802.1Q Management VLAN
-------------	---

Blocage HOL	Prévention du blocage de tête de ligne
-------------	--

Gestion

Interface utilisateur Web	IU Web intégrée pour une configuration basée sur navigateur simplifiée (HTTP/HTTPS)
---------------------------	---

SNMP	SNMP version v1, v2c, v3 avec prise en charge des interceptions.
SNMP MIB	RFC1213 MIB-2, RFC2863 Interface MIB, RFC2665 Ether-like MIB, RFC1493 pont MIB, RFC2674 pont étendu MIB (pont P, pont Q), RFC2819 RMON MIB (groupes 1, 2, 3, 9 uniquement), RFC2737 entité MIB, RFC 2618 client RADIUS MIB RFC interceptions 1215
RMON	L'agent logiciel de surveillance à distance intégré (RMON) prend en charge quatre groupes RMON (historique, statistiques, alarmes et événements) pour une gestion du trafic, une surveillance et une analyse améliorées.
Mise à niveau du micro logiciel	Mise à niveau par le navigateur Web (HTTP) et TFTP
Miroir de port	Le trafic sur un port peut être dupliqué vers un autre port en vue d'une analyse avec un analyseur de réseau ou avec la sonde RMON.
Gestion d'autres éléments	Traceroute Couche d'échange sécurisé (SSL) Secure Shell (SSH) RADIUS miroir de ports Mise à niveau TFTP Sécurité SSL pour IU Web Serveur DHCP BootP SNTP Mise à niveau Xmodem Cable Diagnostics PING Client Telnet (support sécurisé SSH)
Sécurité	
IEEE 802.1x	802.1x - Authentification RADIUS. Cryptage MD5
Contrôle d'accès	ACL - Limite de seuil ou de taux basée sur :

Source et destination basées sur l'adresse MAC
 Adresse IP source et de destination
 Protocole
 TOS/DSCP
 Port
 VLAN
 Ethertype

Disponibilité

Agrégation de liens	Agrégation de liens conformément à la norme IEEE 802.3ad LACP Jusqu'à 8 ports dans 8 groupes au maximum
Contrôle d'avalanche	Diffusion, multidiffusion et diffusion individuelle inconnue
Spanning Tree	Spanning Tree IEEE 802.1D, Rapid Spanning Tree IEEE 802.1w, Multiple Spanning Tree IEEE 802.1s
IGMP Snooping	IGMP Snooping (v1/v2) fournit pour un client rapide des réunions et des départ de flux de multidiffusion et limite le trafic vidéo gourmand en bande passante uniquement vers les demandeurs. Prend en charge 256 groupes de multidiffusion.

QoS (qualité de service)

Niveaux de priorité	4 files d'attente matérielles
Répartition	Formation de files d'attentes par priorité et pondération WRR
Classe de service	basée sur les ports Réseau VLAN 802.1p basé sur la priorité IPv4/v6 IP basé sur la priorité/TOS/DSCP TCP/UDP basé sur les ports Diffserv Classification et marquage des ACL

Limitation du taux	Contrôle de l'entrée Contrôle du taux de sortie
Normes	802.3 Ethernet 10BASE-T, 802.3u Fast Ethernet 100BASE-TX, 802.3ab Gigabit Ethernet 1000BASE-T, 802.3z Gigabit Ethernet, 802.3x contrôle de flux, 802.3 ad LACP, 802.1d STP, 802.1Q/p VLAN, 802.1w Rapid STP, 802.1s Multiple STP, 802.1x authentification d'accès aux ports

Environnement

Dimensions	279 mm x 44 mm x 170 mm
Poids unitaire	1 kg
Alimentation	Adaptateur externe CA
Certifications	FCC Part15 Classe A, CE Classe A, UL, cUL, marque CE, CB
Température de fonctionnement	0 à 40 °C
Température de stockage	-20 à 70 °C
Humidité en fonctionnement	10 à 90 %, non condensée
Humidité de stockage	10 à 95 %, non condensée

SRW208L

Ports	8 connecteurs RJ-45 pour 10/100BASE-TX, 1 port mini GBIC/SFP port et 1 connecteur type LC pour port 100LX SMF à 1 310 nm Port Console Auto MDI/MDI-X Négociation automatique/Paramétrage manuel
-------	--

Type de câblage	UTP CAT 5 ou qualité supérieure pour 10BASE-T/100BASE-TX, UTP CAT 5e ou qualité supérieure pour 1000BASE-T
-----------------	--

DEL	10/100 Link/Act, 1 Gig Link/Act, Speed, 1 100LC Link/Act, System
-----	--

Performances

Capacité de commutation	3,8 Go sans blocage
-------------------------	---------------------

Taux de transfert	Performances de vitesse câblée de 2,8 Mpps
-------------------	--

Couche 2

Taille de table MAC	8 Ko
---------------------	------

Nombre de réseaux VLAN	256 réseaux VLAN actifs (plage de 4096)
------------------------	---

Réseau VLAN	Réseaux VLAN basés sur les ports et le marquage 802.1Q Management VLAN
-------------	---

Blocage HOL	Prévention du blocage de tête de ligne
-------------	--

Gestion

Interface utilisateur Web	IU Web intégrée pour une configuration basée sur navigateur simplifiée (HTTP/HTTPS)
---------------------------	---

SNMP	SNMP version v1, v2c, v3 avec prise en charge des interceptions.
SNMP MIB	RFC1213 MIB-2, RFC2863 Interface MIB, RFC2665 Ether-like MIB, RFC1493 pont MIB, RFC2674 pont étendu MIB (pont P, pont Q), RFC2819 RMON MIB (groupes 1, 2, 3, 9 uniquement), RFC2737 entité MIB, RFC 2618 client RADIUS MIB interceptions RFC 1215
RMON	L'agent logiciel de surveillance à distance intégré (RMON) prend en charge quatre groupes RMON (historique, statistiques, alarmes et événements) pour une gestion du trafic, une surveillance et une analyse améliorées.
Mise à niveau du micro logiciel	Mise à niveau par le navigateur Web (HTTP) et TFTP
Miroir de port	Le trafic sur un port peut être dupliqué vers un autre port en vue d'une analyse avec un analyseur de réseau ou avec la sonde RMON.
Gestion d'autres éléments	Traceroute Couche d'échange sécurisé (SSL) Secure Shell (SSH) RADIUS miroir de ports Mise à niveau TFTP Sécurité SSL pour IU Web Serveur DHCP BootP SNTP Mise à niveau Xmodem Cable Diagnostics PING Client Telnet (support sécurisé SSH)
Sécurité	
IEEE 802.1x	802.1x - Authentification RADIUS. Cryptage MD5

Contrôle d'accès	ACL - Limite de seuil ou de taux basée sur : Source et destination basées sur l'adresse MAC Adresse IP source et de destination Protocole TOS/DSCP Port VLAN Ethertype
-------------------------	---

Disponibilité

Agrégation de liens	Agrégation de liens conformément à la norme IEEE 802.3ad LACP Jusqu'à 8 ports dans 8 groupes au maximum
Contrôle d'avalanche	Diffusion, multidiffusion et diffusion individuelle inconnue
Spanning Tree	Spanning Tree IEEE 802.1D, Rapid Spanning Tree IEEE 802.1w, Multiple Spanning Tree IEEE 802.1s
IGMP Snooping	IGMP Snooping (v1/v2) fournit pour un client rapide des réunions et des départ de flux de multidiffusion et limite le trafic vidéo gourmand en bande passante uniquement vers les demandeurs. Prend en charge 256 groupes de multidiffusion.

QoS (qualité de service)

Niveaux de priorité	4 files d'attente matérielles
Répartition	Formation de files d'attentes par priorité et pondération WRR
Classe de service	basée sur les ports Réseau VLAN 802.1p basé sur la priorité IPv4/v6 IP basé sur la priorité/TOS/DSCP TCP/UDP basé sur les ports Diffserv Classification et marquage des ACL

Limitation du taux	Contrôle de l'entrée Contrôle du taux de sortie
Normes	802.3 Ethernet 10BASE-T, 802.3u Fast Ethernet 100BASE-TX, 802.3ab Gigabit Ethernet 1000BASE-T, 802.3z Gigabit Ethernet, 802.3x contrôle de flux, 802.3 ad LACP, 802.1d STP, 802.1Q/p VLAN, 802.1w Rapid STP, 802.1s Multiple STP, 802.1x authentification d'accès aux ports

Environnement

Dimensions	279 mm x 44 mm x 170 mm
Poids unitaire	1 kg
Alimentation	Adaptateur externe CA
Certifications	FCC Part15 Classe A, CE Classe A, UL, cUL, marque CE, CB
Température de fonctionnement	0 à 40 °C
Température de stockage	-20 à 70 °C
Humidité en fonctionnement	10 à 90 %, non condensée
Humidité de stockage	10 à 95 %, non condensée

SRW208MP

Ports	8 connecteurs RJ-45 pour 10BASE-T et 100BASE-TX, 2 connecteurs RJ-45 pour 10BASE-T/100BASE-TX/1000BASE-T avec 2 emplacements SFP Port Console Auto MDI/MDI-X Négociation automatique/Paramétrage manuel
Type de câblage	UTP CAT 5 ou qualité supérieure pour 10BASE-T/100BASE-TX, UTP CAT 5e ou qualité supérieure pour 1000BASE-T
DEL	10/100 Link/Act, POE, 2 Gig Link/Act, Speed, System
POE 100	Compatible norme 802.3af. Alimente jusqu'à un maximum de 15,4 W, en conformité avec les normes IEEE, sur les ports 8 10/

Performances

Capacité de commutation	5,6 Go sans blocage
Taux de transfert	Performances de vitesse câblée de 4,17 Mpps

Couche 2

Taille de table MAC	8 Ko
Nombre de réseaux VLAN	256 réseaux VLAN actifs (plage de 4096)
Réseau VLAN	Réseaux VLAN basés sur les ports et le marquage 802.1Q Management VLAN
Blocage HOL	Prévention du blocage de tête de ligne

Gestion

Interface utilisateur Web	IU Web intégrée pour une configuration basée sur navigateur simplifiée (HTTP/HTTPS)
SNMP	SNMP version v1, v2c, v3 avec prise en charge des interceptions
SNMP MIB	RFC1213 MIB-2, RFC2863 Interface MIB, RFC2665 Ether-like MIB, RFC1493 pont MIB, RFC2674 pont étendu MIB (pont P, pont Q), RFC2819 RMON MIB (groupes 1, 2, 3, 9 uniquement), RFC2737 entité MIB, RFC 2618 client RADIUS MIB RFC interceptions 1215, MIB POE privé
RMON	L'agent logiciel de surveillance à distance intégré (RMON) prend en charge quatre groupes RMON (historique, statistiques, alarmes et événements) pour une gestion du trafic, une surveillance et une analyse améliorées.
Mise à niveau du micro logiciel	Mise à niveau par le navigateur Web (HTTP) et TFTP
Miroir de port	Le trafic sur un port peut être dupliqué vers un autre port en vue d'une analyse avec un analyseur de réseau ou avec la sonde RMON.
Gestion d'autres éléments	Traceroute Couche d'échange sécurisé (SSL) Secure Shell (SSH) RADIUS miroir de ports Mise à niveau TFTP Sécurité SSL pour IU Web Serveur DHCP BootP SNTP Mise à niveau Xmodem Cable Diagnostics PING Client Telnet (support sécurisé SSH)

Sécurité

IEEE 802.1x 802.1x - Authentification RADIUS. Cryptage MD5

Contrôle d'accès ACL - Limite de seuil ou de taux basée sur :
 Source et destination basées sur l'adresse MAC
 Adresse IP source et de destination
 Protocole
 TOS/DSCP
 Port
 VLAN
 Ethertype

Disponibilité

Agrégation de liens Agrégation de liens conformément à la norme IEEE 802.3ad LACP
 Jusqu'à 8 ports dans 8 groupes au maximum

Contrôle d'avalanche Diffusion, multidiffusion et diffusion individuelle inconnue

Spanning Tree Spanning Tree IEEE 802.1d, Rapid Spanning Tree IEEE 802.1w, Multiple Spanning Tree IEEE 802.1s

IGMP Snooping IGMP snooping (v1/v2) limite le trafic vidéo gourmand en bande passante uniquement vers les demandeurs. Prend en charge 256 groupes de multidiffusion.

QoS (qualité de service)

Niveaux de priorité 4 files d'attente matérielles

Répartition Formation de files d'attentes par priorité et pondération WRR

Classe de service basée sur les ports
 Réseau VLAN 802.1p basé sur la priorité
 IPv4/v6 IP basé sur la priorité/TOS/DSCP

	TCP/UDP basé sur les ports Diffserv Classification et marquage des ACL
Limitation du taux	Contrôle de l'entrée Contrôle du taux de sortie
Normes	802.3 Ethernet 10BASE-T, 802.3u Fast Ethernet 100BASE-TX, 802.3ab Gigabit Ethernet 1000BASE-T, 802.3z Gigabit Ethernet, 802.3x contrôle de flux, 802.3 ad LACP, 802.1d STP, 802.1Q/p VLAN, 802.1w Rapid STP, 802.1s Multiple STP, 802.1x authentification d'accès aux ports

Environnement

Dimensions	279 mm x 44 mm x 170 mm
Poids unitaire	1,2 kg
Alimentation	Adaptateur externe CA
Certifications	FCC Part15 Classe A, CE Classe A, UL, cUL, marque CE, CB
Température de fonctionnement	0 à 40 °C
Température de stockage	-20 à 70 °C
Humidité en fonctionnement	10 à 90 %, non condensée
Humidité de stockage	10 à 95 %, non condensée

SRW208P

Ports	8 connecteurs RJ-45 pour 10BASE-T et 100BASE-TX, 2 connecteurs RJ-45 pour 10BASE-T/100BASE-TX/1000BASE-T avec 2 emplacements SFP Port Console Auto MDI/MDI-X Négociation automatique/Paramétrage manuel
Type de câblage	UTP CAT 5 ou qualité supérieure pour 10BASE-T/100BASE-TX, UTP CAT 5e ou qualité supérieure pour 1000BASE-T
DEL	10/100 Link/Act, POE, 2 Giga Link/Act, Speed, System
POE	Compatible norme 802.3af. Alimente jusqu'à un maximum de 15,4 W sur 4 ports 10/100 ou jusqu'à 7,5 W sur 8 ports 10/100

Performances

Capacité de commutation	5,6 Go sans blocage
Taux de transfert	Performances de vitesse câblée de 4,17 Mpps

Couche 2

Taille de table MAC	8 Ko
Nombre de réseaux VLAN	256 réseaux VLAN actifs (plage de 4096)
Réseau VLAN	Réseaux VLAN basés sur les ports et le marquage 802.1Q Management VLAN
Blocage HOL	Prévention du blocage de tête de ligne

Gestion

Interface utilisateur Web	IU Web intégrée pour une configuration basée sur navigateur simplifiée (HTTP/HTTPS)
SNMP	SNMP version v1, v2c, v3 avec prise en charge des interceptions
SNMP MIB	RFC1213 MIB-2, RFC2863 Interface MIB, RFC2665 Ether-like MIB, RFC1493 pont MIB, RFC2674 pont étendu MIB (pont P, pont Q), RFC2819 RMON MIB (groupes 1, 2, 3, 9 uniquement), RFC2737 entité MIB, RFC 2618 client RADIUS MIB RFC interceptions 1215, MIB POE privé
RMON	L'agent logiciel de surveillance à distance intégré (RMON) prend en charge quatre groupes RMON (historique, statistiques, alarmes et événements) pour une gestion du trafic, une surveillance et une analyse améliorées.
Mise à niveau du micro logiciel	Mise à niveau par le navigateur Web (HTTP) et TFTP
Miroir de port	Le trafic sur un port peut être dupliqué vers un autre port en vue d'une analyse avec un analyseur de réseau ou avec la sonde RMON.
Gestion d'autres éléments	Traceroute Couche d'échange sécurisé (SSL) Secure Shell (SSH) RADIUS miroir de ports Mise à niveau TFTP Sécurité SSL pour IU Web Serveur DHCP BootP SNTP Mise à niveau Xmodem Cable Diagnostics PING Client Telnet (support sécurisé SSH)

Sécurité

IEEE 802.1x 802.1x - Authentification RADIUS. Cryptage MD5

Contrôle d'accès ACL - Limite de seuil ou de taux basée sur :
 Source et destination basées sur l'adresse MAC
 Adresse IP source et de destination
 Protocole
 TOS/DSCP
 Port
 VLAN
 Ethertype

Disponibilité

Agrégation de liens Agrégation de liens conformément à la norme IEEE 802.3ad LACP
 Jusqu'à 8 ports dans 8 groupes au maximum

Contrôle d'avalanche Diffusion, multidiffusion et diffusion individuelle inconnue

Spanning Tree Spanning Tree IEEE 802.1D, Rapid Spanning Tree IEEE 802.1w, Multiple Spanning Tree IEEE 802.1s

IGMP Snooping IGMP Snooping (v1/v2) fournit pour un client rapide des réunions et des départ de flux de multidiffusion et limite le trafic vidéo gourmand en bande passante uniquement vers les demandeurs. Prend en charge 256 groupes de multidiffusion.

QoS (qualité de service)

Niveaux de priorité 4 files d'attente matérielles

Répartition Formation de files d'attentes par priorité et pondération WRR

Classe de service basée sur les ports
 Réseau VLAN 802.1p basé sur la priorité
 IPv4/v6 IP basé sur la priorité/TOS/DSCP

	TCP/UDP basé sur les ports Diffserv Classification et marquage des ACL
Limitation du taux	Contrôle de l'entrée Contrôle du taux de sortie
Normes	802.3 Ethernet 10BASE-T, 802.3u Fast Ethernet 100BASE-TX, 802.3ab Gigabit Ethernet 1000BASE-T, 802.3z Gigabit Ethernet, 802.3x contrôle de flux, 802.3ad LACP, 802.3af POE, 802.1D STP, 802.1Q/p VLAN, 802.1w Rapid STP, 802.1s Multiple STP, 802.1x authentification d'accès aux ports
Environnement	
Dimensions	279 mm x 44 mm x 170 mm
Poids unitaire	1,2 kg
Alimentation	Adaptateur externe CA
Certifications	FCC Part15 Classe A, CE Classe A, UL, cUL, marque CE, CB
Température de fonctionnement	0 à 40 °C
Température de stockage	-20 à 70 °C
Humidité en fonctionnement	10 à 90 %, non condensée
Humidité de stockage	10 à 95 %, non condensée

Annexe F : Garantie

Linksys garantit que vos produits Linksys sont, pour l'essentiel, exempts de vices matériels et de fabrication, sous réserve d'une utilisation normale, pendant une période de trois années consécutives (« Période de garantie »). Votre unique recours et l'entière responsabilité de Linksys sont limités, au choix de Linksys, soit à la réparation ou au remplacement du produit, soit au remboursement du prix à l'achat moins les remises obtenues. Cette garantie limitée concerne uniquement l'acheteur d'origine.

Si ce produit devait s'avérer défectueux pendant cette période de garantie, contactez le support technique de Linksys pour obtenir, si besoin est, un numéro d'autorisation de retour. **N'OUBLIEZ PAS DE CONSERVER VOTRE PREUVE D'ACHAT À PORTÉE DE MAIN LORS DE TOUT CONTACT TÉLÉPHONIQUE.** Si Linksys vous demande de retourner le produit, indiquez lisiblement le numéro d'autorisation de retour à l'extérieur de l'emballage et joignez-y une copie de l'original de votre preuve d'achat. **AUCUNE DEMANDE DE RETOUR NE PEUT ÊTRE TRAITÉE EN L'ABSENCE D'UNE PREUVE D'ACHAT.** Les frais d'expédition des produits défectueux à Linksys sont à votre charge. Linksys prend uniquement en charge les envois via UPS Ground de Linksys chez vous. Les frais d'envoi restent à la charge des clients implantés en dehors des États-Unis et du Canada.

TOUTES LES GARANTIES IMPLICITES ET CONDITIONS DE VALEUR MARCHANDE OU D'ADÉQUATION À UN USAGE PARTICULIER SONT LIMITÉES À LA DURÉE DE LA PÉRIODE DE GARANTIE. TOUTES LES AUTRES CONDITIONS, DÉCLARATIONS ET GARANTIES IMPLICITES OU EXPLICITES, Y COMPRIS TOUTE GARANTIE IMPLICITE DE NON-CONTREFAÇON SONT EXCLUES. Certaines juridictions n'autorisent pas les restrictions relatives à la durée d'une garantie implicite. Par conséquent, la restriction susmentionnée peut ne pas vous être applicable. Cette garantie vous accorde des droits spécifiques. Vous pouvez avoir d'autres droits qui varient en fonction des juridictions.

Cette garantie ne s'applique pas si le produit (a) a été modifié, sauf si cette modification est le fait de Linksys, (b) n'a pas été installé, exploité, réparé ou entretenu conformément aux instructions fournies par Linksys ou (c) a été altéré suite à une charge physique ou électrique anormale, un usage inadapté du produit, une négligence ou un accident. De plus, en raison du développement permanent de nouvelles techniques visant à infiltrer et attaquer les réseaux, Linksys ne garantit pas que le présent produit est protégé contre toute intrusion ou attaque dont vous feriez l'objet.

CONFORMÉMENT À LA LOI ET INDÉPENDAMMENT DU FONDEMENT DE LA RESPONSABILITÉ (Y COMPRIS LES ACTES DE NÉGLIGENCE), LINKSYS NE PEUT EN AUCUN CAS ÊTRE TENU RESPONSABLE DES PERTES DE DONNÉES, DE REVENUS OU DE PROFITS OU DES DOMMAGES SPÉCIAUX, INDIRECTS, CONSÉCUTIFS, ACCIDENTELS OU ACCESSOIRES LIÉS OU NON LIÉS À L'UTILISATION OU À L'INCAPACITÉ À UTILISER LE PRODUIT (Y COMPRIS TOUS LES LOGICIELS), MÊME SI LINKSYS A ÉTÉ AVERTI DE LA POSSIBILITÉ DE TELS DOMMAGES. LA RESPONSABILITÉ DE LINKSYS NE DÉPASSE EN AUCUN CAS LE MONTANT RÉGLÉ PAR VOS SOINS POUR LE PRODUIT. Les restrictions susmentionnées s'appliquent même si toutes les garanties ou les recours stipulés dans le présent contrat ne remplissent pas leur fonction principale. Certaines juridictions n'autorisent pas l'exclusion ou la limitation des dommages accessoires ou fortuits, de telle sorte que la limitation ou l'exclusion susmentionnée peut ne pas vous être applicable.

Cette garantie est valide et peut ne s'appliquer que dans le pays d'acquisition du produit.

Veuillez envoyer toutes vos demandes de renseignement à l'adresse suivante : Linksys, P.O. Box 18558, Irvine, CA 92623, États-Unis.

Annexe G : Réglementation

Déclaration FCC

Ce produit a été testé et déclaré conforme aux spécifications des équipements numériques de catégorie B, établies dans la section 15 des réglementations FCC. L'objectif de ces normes est de fournir une protection raisonnable contre toute interférence nuisible dans une installation résidentielle. Cet équipement génère, utilise et peut émettre de l'énergie à hautes fréquences nuisible et, s'il n'est pas installé et utilisé selon le manuel d'instruction, peut provoquer des interférences gênantes pour les communications radio. Il ne peut toutefois être garanti qu'aucune installation ne causera d'interférences. Si cet équipement provoque des interférences gênantes pour la réception des ondes de radio ou de télévision, détectables en mettant l'équipement hors tension et sous tension, l'utilisateur peut tenter de remédier à ces interférences des façons suivantes :

- Réorientation ou déplacement de l'antenne de réception
- Éloignement de l'équipement ou des périphériques
- Branchement de l'équipement sur une prise différente de celle du récepteur
- Demande d'aide à un revendeur ou technicien radio/télévision expérimenté

Conseils de sécurité

Attention : pour réduire le risque d'incendie, utilisez uniquement un cordon d'alimentation AWG N° 26 ou un cordon d'alimentation de télécommunications de taille plus importante.

N'utilisez pas ce produit à proximité d'eau, par exemple dans un sous-sol humide ou près d'une piscine.

Évitez d'utiliser ce produit pendant un orage. Il pourrait y avoir un risque de choc électrique à cause de la foudre.

Industry Canada (Canada)

Cet appareil est conforme à la norme ICES-003 d'Industry Canada.

Cet appareil est conforme à la norme NMB003 d'Industrie Canada.

IC Statement

Commutateurs WebView

Operation is subject to the following two conditions:

1. This device may not cause interference and
2. This device must accept any interference, including interference that may cause undesired operation of the device.

Règlement d'Industry Canada

Le fonctionnement est soumis aux conditions suivantes :

1. Ce périphérique ne doit pas causer d'interférences ;
2. Ce périphérique doit accepter toutes les interférences reçues, y compris celles qui risquent d'entraîner un fonctionnement indésirable.

Déclaration de conformité CE (Europe)

Conformément à la directive CEM 89/336/CEE, la directive basse tension 73/23/CEE et la directive d'amendement 93/68/CEE, ce produit respecte les normes suivantes :

- EN55022 Émission
- EN55024 Immunité
- EN60950 Sécurité

Informations utilisateur pour les produits grand public couverts par la directive européenne 2002/96/EC sur les déchets électriques et électroniques Équipement (WEEE)

Ce document contient des informations importantes pour les utilisateurs au sujet de la destruction et du recyclage des produits Linksys. Les consommateurs doivent se conformer à cette notice pour tous les produits électroniques portant le symbole suivant :

English

Environmental Information for Customers in the European Union

European Directive 2002/96/EC requires that the equipment bearing this symbol on the product and/or its packaging must not be disposed of with unsorted municipal waste. The symbol indicates that this product should be disposed of separately from regular household waste streams. It is your responsibility to dispose of this and other electric and electronic equipment via designated collection facilities appointed by the government or local authorities. Correct disposal and recycling will help prevent potential negative consequences to the environment and human health. For more detailed information about the disposal of your old equipment, please contact your local authorities, waste disposal service, or the shop where you purchased the product.

Ceština/Czech

Informace o ochraně životního prostředí pro zákazníky v zemích Evropské unie

Evropská směrnice 2002/96/ES zakazuje, aby zařízení označené tímto symbolem na produktu anebo na obalu bylo likvidováno s netříděným komunálním odpadem. Tento symbol udává, že daný produkt musí být likvidován odděleně od běžného komunálního odpadu. Odpovídáte za likvidaci tohoto produktu a dalších elektrických a elektronických zařízení prostřednictvím určených sběrných míst stanovených vládou nebo místními úřady. Správná likvidace a recyklace pomáhá předcházet potenciálním negativním dopadům na životní prostředí a lidské zdraví. Podrobnější informace o likvidaci starého vybavení si laskavě vyžádejte od místních úřadů, podniku zabývajícího se likvidací komunálních odpadů nebo obchodu, kde jste produkt zakoupili.



Dansk/Danish**Miljøinformation for kunder i EU**

EU-direktiv 2002/96/EF kræver, at udstyr der bærer dette symbol på produktet og/eller emballagen ikke må bortskaffes som usorteret kommunalt affald. Symbolet betyder, at dette produkt skal bortskaffes adskilt fra det almindelige husholdningsaffald. Det er dit ansvar at bortskaffe dette og andet elektrisk og elektronisk udstyr via bestemte indsamlingssteder udpeget af staten eller de lokale myndigheder. Korrekt bortskaffelse og genvinding vil hjælpe med til at undgå mulige skader for miljøet og menneskers sundhed. Kontakt venligst de lokale myndigheder, renovationstjenesten eller den butik, hvor du har købt produktet, angående mere detaljeret information om bortskaffelse af dit gamle udstyr.

Deutsch/German**Umweltinformation für Kunden innerhalb der Europäischen Union**

Die Europäische Richtlinie 2002/96/EC verlangt, dass technische Ausrüstung, die direkt am Gerät und/oder an der Verpackung mit diesem Symbol versehen ist nicht zusammen mit unsortiertem Gemeindeabfall entsorgt werden darf. Das Symbol weist darauf hin, dass das Produkt von regulärem Haushaltsmüll getrennt entsorgt werden sollte. Es liegt in Ihrer Verantwortung, dieses Gerät und andere elektrische und elektronische Geräte über die dafür zuständigen und von der Regierung oder örtlichen Behörden dazu bestimmten Sammelstellen zu entsorgen. Ordnungsgemäßes Entsorgen und Recyceln trägt dazu bei, potentielle negative Folgen für Umwelt und die menschliche Gesundheit zu vermeiden. Wenn Sie weitere Informationen zur Entsorgung Ihrer Altgeräte benötigen, wenden Sie sich bitte an die örtlichen Behörden oder städtischen Entsorgungsdienste oder an den Händler, bei dem Sie das Produkt erworben haben.

Eesti/Estonian**Keskkonnaalane informatsioon Euroopa Liidus asuvatele klientidele**

Euroopa Liidu direktiivi 2002/96/EÜ nõuete kohaselt on seadmeid, millel on tootet või pakendil käesolev sümbol, keelatud kõrvaldada koos sorteerimata olmejäätmetega. See sümbol näitab, et toode tuleks kõrvaldada eraldi tavalistest olmejäätmevoogudest. Olete kohustatud kõrvaldama käesoleva ja ka muud elektri- ja elektroonikaseadmed riigi või kohalike ametiasutuste poolt ette nähtud kogumispunktide kaudu. Seadmete korrektne kõrvaldamine ja ringlussevõtt aitab vältida võimalikke negatiivseid tagajärgi keskkonnale ning inimeste tervisele. Vanade seadmete kõrvaldamise kohta täpsema informatsiooni saamiseks võtke palun ühendust kohalike ametiasutustega, jäätmekäitlusfirmaga või kauplusega, kust te toote ostsite.

Español/Spanish**Información medioambiental para clientes de la Unión Europea**

La Directiva 2002/96/CE de la UE exige que los equipos que lleven este símbolo en el propio aparato y/o en su embalaje no deben eliminarse junto con otros residuos urbanos no seleccionados. El símbolo indica que el producto en cuestión debe separarse de los residuos domésticos convencionales con vistas a su eliminación. Es responsabilidad suya desechar este y cualesquiera otros aparatos eléctricos y electrónicos a través de los puntos de recogida que ponen a su disposición el gobierno y las autoridades locales. Al desechar y reciclar correctamente estos aparatos estará contribuyendo a evitar posibles consecuencias negativas para el medio ambiente y la salud de las personas. Si desea obtener información más detallada sobre la eliminación segura de su aparato usado, consulte a las autoridades locales, al servicio de recogida y eliminación de residuos de su zona o pregunte en la tienda donde adquirió el producto.

Ελληνικά/Greek**Στοιχεία περιβαλλοντικής προστασίας για πελάτες εντός της Ευρωπαϊκής Ένωσης**

Η Κοινοτική Οδηγία 2002/96/EC απαιτεί ότι ο εξοπλισμός, ο οποίος φέρει αυτό το σύμβολο στο προϊόν και/ή στη συσκευασία του δεν πρέπει να απορρίπτεται μαζί με τα μικτά κοινотικά απορρίμματα. Το σύμβολο υποδεικνύει ότι αυτό το προϊόν θα πρέπει να απορρίπτεται ξεχωριστά από τα συνήθη οικιακά απορρίμματα. Είστε υπεύθυνος για την απόρριψη του παρόντος και άλλου ηλεκτρικού και ηλεκτρονικού εξοπλισμού μέσω των καθορισμένων εγκαταστάσεων συγκέντρωσης απορριμμάτων οι οποίες παρέχονται από το κράτος ή τις αρμόδιες τοπικές αρχές. Η σωστή απόρριψη και ανακύκλωση συμβάλλει στην πρόληψη πιθανών αρνητικών συνεπειών για το περιβάλλον και την υγεία. Για περισσότερες πληροφορίες σχετικά με την απόρριψη του παλιού σας εξοπλισμού, παρακαλώ επικοινωνήστε με τις τοπικές αρχές, τις υπηρεσίες απόρριψης ή το κατάστημα από το οποίο αγοράσατε το προϊόν.

Français/French

Informations environnementales pour les clients de l'Union européenne

La directive européenne 2002/96/CE exige que l'équipement sur lequel est apposé ce symbole sur le produit et/ou son emballage ne soit pas jeté avec les autres ordures ménagères. Ce symbole indique que le produit doit être éliminé dans un circuit distinct de celui pour les déchets des ménages. Il est de votre responsabilité de jeter ce matériel ainsi que tout autre matériel électrique ou électronique par les moyens de collecte indiqués par le gouvernement et les pouvoirs publics des collectivités territoriales. L'élimination et le recyclage en bonne et due forme ont pour but de lutter contre l'impact néfaste potentiel de ce type de produits sur l'environnement et la santé publique. Pour plus d'informations sur le mode d'élimination de votre ancien équipement, veuillez prendre contact avec les pouvoirs publics locaux, le service de traitement des déchets, ou l'endroit où vous avez acheté le produit.

Italiano/Italian

Informazioni relative all'ambiente per i clienti residenti nell'Unione Europea

La direttiva europea 2002/96/EC richiede che le apparecchiature contrassegnate con questo simbolo sul prodotto e/o sull'imballaggio non siano smaltite insieme ai rifiuti urbani non differenziati. Il simbolo indica che questo prodotto non deve essere smaltito insieme ai normali rifiuti domestici. È responsabilità del proprietario smaltire sia questi prodotti sia le altre apparecchiature elettriche ed elettroniche mediante le specifiche strutture di raccolta indicate dal governo o dagli enti pubblici locali. Il corretto smaltimento ed il riciclaggio aiuteranno a prevenire conseguenze potenzialmente negative per l'ambiente e per la salute dell'essere umano. Per ricevere informazioni più dettagliate circa lo smaltimento delle vecchie apparecchiature in Vostro possesso, Vi invitiamo a contattare gli enti pubblici di competenza, il servizio di smaltimento rifiuti o il negozio nel quale avete acquistato il prodotto.

Latviešu valoda/Latvian

Ekoloģiska informācija klientiem Eiropas Savienības jurisdikcijā

Direktīvā 2002/96/EK ir prasība, ka aprīkojumu, kam pievienota zīme uz paša izstrādājuma vai uz tā iesaiņojuma, nedrīkst izmest nešķīrotā veidā kopā ar komunālajiem atkritumiem (tiem, ko rada vietēji iedzīvotāji un uzņēmumi). Šī zīme nozīmē to, ka šī ierīce ir jāizmet atkritumos tā, lai tā nenonāktu kopā ar parastiem mājāsaimniecības atkritumiem. Jūsu pienākums ir šo un citas elektriskās un elektroniskās ierīces izmest atkritumos, izmantojot īpašus atkritumu savākšanas veidus un līdzekļus, ko nodrošina valsts un pašvaldību iestādes. Ja izmestā atkritumos un pārstrāde tiek veikta pareizi, tad mazinās iespējamais kaitējums dabai un cilvēku veselībai. Sīkākas ziņas par novecojušu aprīkojuma izmešanu atkritumos jūs varat saņemt vietējā pašvaldībā, atkritumu savākšanas dienestā, kā arī veikalā, kur iegādājāties šo izstrādājumu.

Lietuvškai/Lithuanian

Aplinkosaugos informacija, skirta Europos Sąjungos vartotojams

Europos direktyva 2002/96/EC numato, kad įrangos, kuri ir (arba) kurios pakuotė yra pažymėta šiuo simboliu, negalima šalinti kartu su nerūšiuotomis komunalinėmis atliekomis. Šis simbolis rodo, kad gaminį reikia šalinti atskirai nuo bendro buitinių atliekų srauto. Jūs privalote užtikrinti, kad ši ir kita elektros ar elektroninė įranga būtų šalinama per tam tikras nacionalinės ar vietinės valdžios nustatytas atliekų rinkimo sistemas. Tinkamai šalinant ir perdurbant atliekas, bus išvengta galimos žalos aplinkai ir žmonių sveikatai. Daugiau informacijos apie jūsų senos įrangos šalinimą gali pateikti vietinės valdžios institucijos, atliekų šalinimo tarnybos arba parduotuvės, kuriose įsigijote tą gaminį.

Malti/Maltese

Informazzjoni Ambjentali għal Kliġenti fl-Unjoni Ewropea

Id-Direttiva Ewropea 2002/96/KE titlob li t-tagħmir li jkun fih is-simbolu fuq il-prodott u/jew fuq l-ippakkjar ma jistax jintrema ma' skart municipli li ma għex isseparat. Is-simbolu jindika li dan il-prodott għandu jintrema separatament minn ma' l-iskart domestiku regolari. Hija responsabbiltà tiegħek li tarmi dan it-tagħmir u kull tagħmir iehor ta' l-elettriku u elettroniku permezz ta' faċilitajiet ta' għbir appuntati apposta mill-gvern jew mill-awtoritajiet lokali. Ir-rimi b'mod korrett u r-riciklaġġ jghin jipprevjeni konsegwenzi negattivi potenzjali għall-ambjent u għas-saħħa tal-bniedem. Għal aktar informazzjoni dettaljata dwar ir-rimi tat-tagħmir antik tiegħek, jekk jogħġbok ikkuntattja lill-awtoritajiet lokali tiegħek, is-servizzi għar-rimi ta' l-iskart, jew il-hanut minn fejn xtrajt il-prodott.

Magyar/Hungarian

Környezetvédelmi információ az európai uniós vásárlók számára

A 2002/96/EC számú európai uniós irányelv megkívánja, hogy azokat a termékeket, amelyeken, és/vagy amelyek csomagolásán az alábbi címke megjelenik, tilos a többi szelektálatlan lakossági hulladékkal együtt kidobni. A címke azt jelöli, hogy az adott termék kidobásakor a szokványos háztartási hulladékelszállítási rendszerektől elkülönített eljárást kell alkalmazni. Az Ön felelőssége, hogy ezt, és más elektromos és elektronikus berendezéseit a kormányzati vagy a helyi hatóságok által kijelölt gyűjtőrendszeren keresztül számolja fel. A megfelelő hulladékfeldolgozás segít a környezetre és az emberi egészségre potenciálisan ártalmas negatív hatások megelőzésében. Ha elavult berendezéseinek felszámolásához további részletes információra van szüksége, kérjük, lépjen kapcsolatba a helyi hatóságokkal, a hulladékfeldolgozási szolgálattal, vagy azzal üzlettel, ahol a terméket vásárolta.

Nederlands/Dutch

Milieu-informatie voor klanten in de Europese Unie

De Europese Richtlijn 2002/96/EC schrijft voor dat apparatuur die is voorzien van dit symbool op het product of de verpakking, niet mag worden ingezameld met niet-gescheiden huishoudelijk afval. Dit symbool geeft aan dat het product apart moet worden ingezameld. U bent zelf verantwoordelijk voor de vernietiging van deze en andere elektrische en elektronische apparatuur via de daarvoor door de landelijke of plaatselijke overheid aangewezen inzamelingskanalen. De juiste vernietiging en recycling van deze apparatuur voorkomt mogelijke negatieve gevolgen voor het milieu en de gezondheid. Voor meer informatie over het vernietigen van uw oude apparatuur neemt u contact op met de plaatselijke autoriteiten of afvalverwerkingsdienst, of met de winkel waar u het product hebt aangeschaft.

Norsk/Norwegian

Miljøinformasjon for kunder i EU

EU-direktiv 2002/96/EF krever at utstyr med følgende symbol avbildet på produktet og/eller pakningen, ikke må kastes sammen med usortert avfall. Symbolet indikerer at dette produktet skal håndteres atskilt fra ordinær avfallsinnsamling for husholdningsavfall. Det er ditt ansvar å kvitte deg med dette produktet og annet elektrisk og elektronisk avfall via egne innsamlingsordninger slik myndighetene eller kommunene bestemmer. Korrekt avfallshåndtering og gjenvinning vil være med på å forhindre mulige negative konsekvenser for miljø og helse. For nærmere informasjon om håndtering av det kasserte utstyret ditt, kan du ta kontakt med kommunen, en innsamlingsstasjon for avfall eller butikken der du kjøpte produktet.

Polski/Polish

Informacja dla klientów w Unii Europejskiej o przepisach dotyczących ochrony środowiska

Dyrektywa Europejska 2002/96/EC wymaga, aby sprzęt oznaczony symbolem znajdującym się na produkcie i/lub jego opakowaniu nie był wyrzucany razem z innymi niesortowanymi odpadami komunalnymi. Symbol ten wskazuje, że produkt nie powinien być usuwany razem ze zwykłymi odpadami z gospodarstw domowych. Na Państwie spoczywa obowiązek wyrzucania tego i innych urządzeń elektrycznych oraz elektronicznych w punktach odbioru wyznaczonych przez władze krajowe lub lokalne. Pozbywanie się sprzętu we właściwy sposób i jego recykling pomogą zapobiec potencjalnie negatywnym konsekwencjom dla środowiska i zdrowia ludzkiego. W celu uzyskania szczegółowych informacji o usuwaniu starego sprzętu, prosimy zwrócić się do lokalnych władz, służb oczyszczania miasta lub sklepu, w którym produkt został nabyty.

Português/Portuguese

Informação ambiental para clientes da União Europeia

A Directiva Europeia 2002/96/CE exige que o equipamento que exibe este símbolo no produto e/ou na sua embalagem não seja eliminado junto com os resíduos municipais não separados. O símbolo indica que este produto deve ser eliminado separadamente dos resíduos domésticos regulares. É da sua responsabilidade eliminar este e qualquer outro equipamento eléctrico e electrónico através das instalações de recolha designadas pelas autoridades governamentais ou locais. A eliminação e reciclagem correctas ajudarão a prevenir as consequências negativas para o ambiente e para a saúde humana. Para obter informações mais detalhadas sobre a forma de eliminar o seu equipamento antigo, contacte as autoridades locais, os serviços de eliminação de resíduos ou o estabelecimento comercial onde adquiriu o produto.

Slovenčina/Slovak

Informácie o ochrane životného prostredia pre zákazníkov v Európskej únii

Podľa európskej smernice 2002/96/ES zariadenie s týmto symbolom na produkte a/alebo jeho balení nesmie byť likvidované spolu s netriedeným komunálnym odpadom. Symbol znamená, že produkt by sa mal likvidovať oddelene od bežného odpadu z domácnosti. Je vašou povinnosťou likvidovať toto i ostatné elektrické a elektronické zariadenia prostredníctvom špecializovaných zberných zariadení určených vládou alebo miestnymi orgánmi. Správna likvidácia a recyklácia pomôže zabrániť prípadným negatívnym dopadom na životné prostredie a zdravie ľudí. Ak máte záujem o podrobnejšie informácie o likvidácii starého zariadenia, obráťte sa, prosím, na miestne orgány, organizácie zaoberajúce sa likvidáciou odpadov alebo obchod, v ktorom ste si produkt zakúpili.

Slovenčina/Slovene

Okoljske informacije za stranke v Evropski uniji

Evropska direktiva 2002/96/EC prepoveduje odlaganje opreme, označene s tem simbolom – na izdelku in/ali na embalaži – med običajne, nerazvrščene odpadke. Ta simbol opozarja, da je treba izdelek odvreči ločeno od preostalih gospodinskih odpadkov. Vaša odgovornost je, da to in preostalo električno in elektronsko opremo odnesete na posebna zbirališča, ki jih določijo državne ustanove ali lokalna uprava. S pravilnim odlaganjem in recikliranjem boste preprečili morebitne škodljive vplive na okolje in zdravje ljudi. Če želite izvedeti več o odlaganju stare opreme, se obrnite na lokalno upravo, odpad ali trgovino, kjer ste izdelek kupili.

Suomi/Finnish

Ympäristöä koskevia tietoja EU-alueen asiakkaille

EU-direktiivi 2002/96/EY edellyttää, että jos laitteistossa on tämä symboli itse tuotteessa ja/tai sen pakkauksessa, laitteistoa ei saa hävittää lajittelemattoman yhdyskuntajätteen mukana. Symboli merkitsee sitä, että tämä tuote on hävitettävä erillään tavallisesta kotitalousjätteestä. Sinun vastuullasi on hävittää tämä elektroniikkatuote ja muut vastaavat elektroniikkatuotteet viemällä tuote tai tuotteet viranomaisten määräämään keräyspisteeseen. Laitteiston oikea hävittäminen estää mahdolliset kielteiset vaikutukset ympäristöön ja ihmisten terveyteen. Lisätietoja vanhan laitteiston oikeasta hävitystavasta saa paikallisilta viranomaisilta, jätteenhävityspalvelusta tai siitä myymälästä, josta ostit tuotteen.

Svenska/Swedish

Miljöinformation för kunder i Europeiska unionen

Det europeiska direktivet 2002/96/EC kräver att utrustning med denna symbol på produkten och/eller förpackningen inte får kastas med osorterat kommunalt avfall. Symbolen visar att denna produkt bör kastas efter att den avskiljts från vanligt hushållsavfall. Det faller på ditt ansvar att kasta denna och annan elektrisk och elektronisk utrustning på fastställda samlingsplatser utsedda av regeringen eller lokala myndigheter. Korrekt kassering och återvinning skyddar mot eventuella negativa konsekvenser för miljön och personhälsa. För mer detaljerad information om kassering av din gamla utrustning kontaktar du dina lokala myndigheter, avfallshanteringen eller butiken där du köpte produkten.

Pour plus d'informations, visitez www.linksys.com/international.

Annexe H : Contacts

Besoin de contacter Linksys ?

Consultez notre site Web pour obtenir des informations sur les derniers produits et les mises à jour disponibles pour vos produits existants à l'adresse suivante :

<http://www.linksys.com/international>

Si vous rencontrez des problèmes avec un produit Linksys, adressez un e-mail à l'adresse suivante :

En Europe	Adresse e-mail
Allemagne	support.de@linksys.com
Autriche	support.at@linksys.com
Belgique	support.be@linksys.com
Danemark	support.dk@linksys.com
Espagne	support.es@linksys.com
Finlande	support.fi@linksys.com
France	support.fr@linksys.com
Grèce	support.gr@linksys.com (anglais uniquement)
Hongrie	support.hu@linksys.com
Irlande	support.ie@linksys.com
Italie	support.it@linksys.com
Norvège	support.no@linksys.com
Pays-Bas	support.nl@linksys.com
Pologne	support.pl@linksys.com
Portugal	support.pt@linksys.com
République tchèque	support.cz@linksys.com
Royaume-Uni	support.uk@linksys.com

En Europe	Adresse e-mail
Russie	support.ru@linksys.com
Suède	support.se@linksys.com
Suisse	support.ch@linksys.com
Turquie	support.tk@linksys.com

En dehors de l'Europe	Adresse e-mail
Afrique du Sud	support.ze@linksys.com (anglais uniquement)
Amérique latine	support.portuguese@linksys.com ou support.spanish@linksys.com
Asie Pacifique	asiasupport@linksys.com (anglais uniquement)
Émirats Arabes Unis	support.ae@linksys.com (anglais uniquement)
États-Unis et Canada	support@linksys.com
Moyen Orient & Afrique	support.mea@linksys.com (anglais uniquement)

Remarque : pour certains pays, le support technique n'est disponible qu'en anglais.