GUIDE D'ADMINISTRATION

Gamme Cisco SRP500 Plates-formes prêtes pour les services
(Modèles SRP520-U et SRP540)

Cisco et le logo Cisco sont des marques déposées de Cisco Systems, Inc. et/ou de ses sociétés affiliées aux États-Unis et dans d'autres pays. Vous trouverez une liste des marques commerciales de Cisco sur la page Web **www.cisco.com/go/trademarks**. Les autres marques commerciales mentionnées dans les présentes sont la propriété de leurs détenteurs respectifs. Le mot « partenaire » n'implique nullement une relation de partenariat entre Cisco et toute autre entreprise. (1005R)

© 2012 Cisco Systems, Inc. Tous droits réservés.

OL-25930-01

Table des matières

Chapitre 1 : Présentation des plates-formes prêtes pour les services de la gamme SRP500 12

Fonctionnalités du produit 12

Présentation du produit 13

Numéros de modèle 13

Panneau avant (modèles SRP520-U) 14

Panneau avant SRP521W-U 14

Panneau avant SRP526W-U et SRP527W-U 15

Voyants de la façade 15

Panneau avant (modèles SRP540) 16

Façade du modèle SRP541W 16

Panneau avant SRP546W / SRP547W 16

Voyants de la façade 17

Panneau arrière (modèles SRP520-U) 18

Panneau arrière SRP521W-U 18

Panneau arrière SRP526W-U et SRP527W-U 18

Panneau arrière (modèles SRP540) 20

Panneau arrière du modèle SRP541W 20

Panneau arrière SRP546W et SRP547W 20

Vue latérale (modèles SRP520-U) 22

Vue latérale (modèles SRP540) 23

Vue du dessus (modèles SRP520-U) 24

Paramètres par défaut 25

Chapitre 2 : Mise en route à l'aide de l'utilitaire de configuration 26

Connexion à l'utilitaire de configuration 26

Présentation de l'interface de l'utilitaire de configuration 27

Barre de menu principal 27

Icônes 28

Chapitre 3 : Le menu Quick Setup 29

Installation de la configuration de base 29

Configuration WAN (Ethernet) 29

Configuration WAN (ADSL) 30

Configuration LAN 30
Configuration sans fil 31
TR-069 (mise en service à distance) 31
Comptes invité au réseau 32
Configuration avancée 32
Voix 32
Configuration de réseau mobile 32
Pare-feu 32
NAT 33
Redirection d'une plage de ports 33

Chapitre 4 : Configuration des interfaces des plates-formes prêtes pour les services 34

Configuration des interfaces WAN 34
Page Internet Setup 35
Ajout d'une sous-interface 38
Sous-interface Ethernet 38
Paramètres d'encapsulation 41
Paramètres IPoA 41
Paramètres PPPoE 42
Paramètres PPPoA 43
EoA RFC 1483 Bridged 44
Paramètres d'encapsulation DSL communs 44
Page Internet Option 45
Page Mobile Network 46
Page Multi-WAN Configuration 51
Configuration des interfaces VLAN et des ports LAN 54
Page DHCP Server 54
Page VLAN Settings 58
Page Port Settings 60
Page Protocole Spanning Tree Protocol 62
Configuration d'un LAN sans fil 64
Page Basic Wireless Settings 65

Page Wi-Fi Protected Setup 71
Méthodes Wi-Fi 72
Méthode Wi-Fi Protected Setup 1 72
Méthode Wi-Fi Protected Setup 2 72
Méthode Wi-Fi Protected Setup 3 72
Page Wireless MAC Filter 73
Page Advanced Wireless Settings 74
Page Wi-Fi Multimedia Setting 77
Utilisation de l'interface de gestion 77

Chapitre 5 : Configuration du réseau 79

Routage 80
Page Static Routes 80
Page Routing Information Protocol 81
Page Intervlan Routing 83
Page Policy Routing 84
Traduction d'adresses de réseau (NAT) 85
Page Global Settings 86
Page NAT Bypass 87
Page Port Forwarding 88
Page Port Range Triggering 90
Qualité de service 92
Page QoS Bandwidth Control 92
Page QoS Policy 94
Page CoS To Queue 97
Page DSCP To Queue 98
Firewall 99
Page Firewall Filter 99
Page Internet Access Control 101
Page Advanced Firewall Settings 104
Relais PPPoE 107
DNS dynamique 108

Configuration DMZ 110
Page Software DMZ 110
Page Hardware DMZ 111
Protocole de gestion des groupes Internet (IGMP) 112
Universal Plug and Play 113
Cisco Discovery Protocol 114
Réseau invité 115
Page Basic Configuration 115
Page User Account 117
Personnalisation de la page d'accueil 118
Usurpation d'adresse DNS 120

Chapitre 6 : Configuration de la voix 122

Configuration des Services Voix 122
Fonctionnement des ports voix 122
Fonctionnalités voix de la SRP 123
Codecs pris en charge 123
Redondance du proxy SIP 124
Autres fonctionnalités voix de la SRP 125
Enregistrement auprès du prestataire de services. 131
Gestion des services d'identification de l'appelant 132
Optimisation des taux d'aboutissement des télécopies 135
Résolution des problèmes liés au fax 136
Configuration des plans de numérotation 137
À propos des plans de numérotation 137
Séquences de chiffres 137
Exemples de séquence de chiffres 140
Réception et transmission des chiffres composés 142
Temporisateur du plan de numérotation (temporisateur de décrochage) 143
Syntaxe du temporisateur du plan de numérotation 143
Exemples de temporisateur du plan de numérotation 144
Temporisateur long inter-chiffres (temporisateur de saisie incomplète) 144
Syntaxe du temporisateur long inter-chiffres 145
Exemple de temporisateur long inter-chiffres 145
Temporisateur court inter-chiffres (temporisateur de saisie complète) 145

Syntaxe du temporisateur court inter-chiffres 145
Exemples de temporisateurs court inter-chiffres 146
Modification des plans de numérotation 146
Saisie du plan de numérotation de l'interface de ligne 146
Réinitialisation des temporisateurs de contrôle 147
Implémentation d'appel sécurisé 147
Activation des appels sécurisés 147
Détails des appels sécurisés 148
Utilisation d'un Mini-certificat 149
Génération d'un mini certificat 150
Configuration des paramètres de voix 151
Page Info 152
Informations produit 152
État du système 152
État de la ligne 153
État de la ligne PSTN (SRP540 uniquement) 155
Page System 155
Section Divers 156
Section Miscellaneous 156
Page SIP 156
Paramètres SIP 157
Valeurs du minuteur SIP 159
Traitement des codes d'état de réponse 161
Paramètres RTP 162
Types de données utiles SDP 164
Paramètres de prise en charge NAT 165
Page Provisioning 168
Profil de configuration 168
Mise à niveau du microprogramme 172
Paramètres généraux 173
Page Regional 173
Définition des scripts de sonnerie, de cadence et de tonalité 174
Tonalités de progression d'appel 176
Modèles de sonneries distinctes 178
Modèles distincts de tonalité d'appel en attente 179
Noms distincts de modèles de CWT/sonnerie 180
Valeurs de minuteur de contrôle 182
Codes d'activation du service vertical 184
Codes d'annonce du service vertical 190

Codes de sélection des codecs des appels vers l'extérieur 190
Miscellaneous 191
Pages Line (1-4) 194
Line Enable 194
Streaming Audio Server 195
Paramètres NAT 197
Paramètres réseau 197
Paramètres SIP 199
Paramètres de la fonctionnalité d'appel 203
Proxy et enregistrement 204
Informations sur l'abonné 206
Abonnement à un service supplémentaire 207
Configuration audio 210
Plan de numérotation 215
Configuration de la polarité du port FXS 216
Page PSTN (modèles SRP540 uniquement) 217
Activation de ligne PSTN 217
Paramètres SIP 218
Paramètres de sonnerie 218
Valeurs du minuteur PSTN 218
Détection de la déconnexion PSTN 219
Paramètres internationaux 222
Pages User 224
Paramètres de transfert d'appel 225
Paramètres de transfert d'appel sélectif 225
Paramètres de numérotation abrégée 226
Paramètres de service supplémentaire 226
Paramètres de sonnerie distincts 228
Paramètres de sonnerie 228

Chapitre 7 : Configuration VPN 229

VPN IPSec de site à site 229
Page NAT Traversal 229
Page IKE Policy 230
Page IPSec Policy 232
Tunnel GRE 235
Transfert VPN 237

Serveur Cisco VPN 238
Page Users 241

Chapitre 8 : Paramètres d'administration 242

Page Web Access Management 243
Page Remote Support 244
Gestion à distance 245
Page TR-069 246
Page SNMP 248
Description des ports SNMP 249
Page Local TFTP 250
Page Certificate Management 251
Page Time Setup 253
Gestion des utilisateurs 255
Page Password Complexity Settings 255
Page User List 256
Page User Privilege Control 257
Consignation 258
Page Log Setting 258
Page Log module 260
Page Log Viewer 260
Page Firewall Log 261
Page Factory Defaults 262
Page Firmware Upgrade 263
Sauvegarde et restauration des paramètres 263
Page Default Configuration 264
Page Backup Configuration 264
Page Restore Configuration 265
Page Configuration XML 265
Page Reboot 266

Paramètres de commutation 266
Page Jumbo Setting 266
Page Port Status 267
Page DSL Switch Setting 267
Page MAC Filtering (modèles SRP540 uniquement) 267
Status 268

Chapitre 9 : Utilisation des diagnostics de plates-formes prête pour les services 269

Page Ping Test 269
Page Traceroute 270
Page Detect Active LAN Client 270
Page TCP Dump 271
Page ATM Ping OAM 272

Chapitre 10 : Affichage de l'état des plate-formes prêtes pour les services 273

Page Router Status 274
Page Firewall Status 274
Page Interface Information 276
Page Port Statistics 277
Page Wireless Network Status 278
Page Wireless Client Information 278
Page Guest Network Information 279
Page Mobile Network Status 279
Page DHCP Pool Information 282
Page QoS Status 282
Page Routing Table 283
Page ARP Table 284
Page RIP Status 284
Pager IGMP Status 284

Page VPN Status 285
Page VPN Server Status 285
Page CDP Neighbor Information 286
Page Status ADSL 287
Page ADSL Status 287
Page PVC Status 288
Page STP Status 289

Appendix A : Spécifications 290

Appendix B : Pour en savoir plus 292

1

Présentation des plates-formes prêtes pour les services de la gamme SRP500

Merci d'avoir choisi la plate-forme prête pour les services (SRP) de la gamme Cisco SRP500. La gamme SRP500 est constituée de périphériques souples qui permettent aux petites entreprises de se connecter à divers services (données de haute qualité, service voix hébergé, services de sécurité) offerts par des fournisseurs d'accès.

Ce chapitre fournit des informations pour vous familiariser avec le produit. Il comprend les sections suivantes :

- **Fonctionnalités du produit**
- **Présentation du produit**

Pour obtenir des informations sur la manière d'installer physiquement le SRP, reportez-vous aux guides de démarrage rapide des plates-formes Cisco SRP500 prêtes pour les services à l'adresse suivante : www.cisco.com/go/srp500resources.

Fonctionnalités du produit

La gamme Cisco SRP500 offre les fonctions suivantes :

- Intelligence pour la prise en charge des services vocaux de données, de sécurité et d'applications.
- Pile SIP (Session Initiation Protocol, protocole d'initiation de session) de pointe pour fournir des services vocaux clair,s et de grande qualité.
- Interopérabilité avec les passerelles vocales et commutateurs logiciels courants.
- Sécurité intégrée, capacités VPN et un point d'accès sans fil 802.11n.
- Connectivité WAN multiple résiliente.

- Prise en charge des modems de réseau de données mobiles standard USB utilisés pour la sauvegarde de la connectivité et l'équilibrage de charge.
- Mise en service basée sur des normes utilisant TR-069 et TR-104, ou sur l'API XML Cisco pour des déploiements rationalisés.

Présentation du produit

Cette section répertorie les modèles disponibles pour vous aider à vous familiariser avec votre produit SRP, et affiche également le panneau avant, le panneau arrière et la vue latérale pour chaque gamme de produits.

Numéros de modèle

Modèles SRP520-U

Modèle	Description
SRP521W-U	WAN Fast Ethernet 2 ports de téléphone (FXS), 1 port de ligne de basculement (FXO), 1 port WAN (10/100), 4 ports LAN (10/100), 1 ports USB 2.0, 802.11n et WPS (Wi-Fi Protected Setup)
SRP526W-U	ADSL2+ Annexe B (ADSL sur RNIS) 2 ports téléphoniques (FXS), 1 port de ligne de basculement (FXO), 1 port DSL, 4 ports LAN (10/100), 1 port USB 2.0, 802.11n et WPS (Wi-Fi Protected Setup)
SRP527W-U	ADSL2+ Annexe A/M (ADSL sur POTS) 2 ports téléphoniques (FXS), 1 port de ligne de basculement (FXO), 1 port DSL, 4 ports LAN (10/100), 1 port USB 2.0, 802.11n et WPS (Wi-Fi Protected Setup)

Modèles SRP540

Modèle	Description
SRP541W	WAN Gigabit Ethernet 4 ports téléphoniques (FXS), 1 port de ligne (FXO), 2 ports WAN Gigabit, 4 ports Gigabit LAN, 2 ports USB 2.0, 802.11b/g/n et WPS (Wi-fi Protected Setup)
SRP546W	ADSL2+ Annexe B (ADSL sur RNIS) 4 ports téléphoniques (FXS), 1 port de ligne (FXO), 1 port DSL, 1 port Gigabit WAN 4 ports Gigabit LAN 2 ports USB 2.0, 802.11b/g/n et WPS (WiFi Protected Setup)
SRP547W	ADSL2+ Annexe A/M (ADSL sur POTS) 4 ports téléphoniques (FXS), 1 port de ligne (FXO), 1 port DSL, 1 port Gigabit WAN 4 ports Gigabit LAN 2 ports USB 2.0, 802.11b/g/n et WPS (WiFi Protected Setup)

Panneau avant (modèles SRP520-U)

Panneau avant SRP521W-U

Panneau avant SRP526W-U et SRP527W-U

Voyants de la façade

Le tableau suivant décrit les voyants situés sur le panneau avant des modèles SRP520. Ces voyants permettent de surveiller l'activité du système.

Voyants du panneau avant - SRP520-U

Lumières	Description
POWER/SYS	Vert fixe lorsque le SRP a démarré et qu'il est prêt à être utilisé. Clignote en vert pendant le démarrage.
Ports LAN (1–4)	Vert fixe lorsqu'une liaison est établie. Clignote en vert en présence d'activité sur le port LAN.
Port WAN (SRP521W-U uniquement)	Vert fixe lorsqu'une liaison Ethernet est établie. Clignote en vert en présence d'activité sur le port WAN.
Ports téléphoniques (FXS) (1–2)	Vert fixe lorsque le port est connecté à un téléphone ou un télécopieur et que le SRP est en mesure d'effectuer et de recevoir des appels. Clignote en vert lorsqu'il y a un appel en cours sur le port.
DSL CD (SRP526W-U/527W-U)	Clignote en vert lorsqu'un service DSL est détecté. Vert fixe une fois la synchronisation effectuée.
DSL Data (SRP526W-U/527W-U)	Clignote en vert en présence d'activité DSL sur la ligne.
WLAN	Vert fixe lorsque la radio est sous tension et opérationnelle. Clignote en vert en présence d'activité sans fil sur le port WLAN.

(Suite) Voyants du panneau avant - SRP520-U

Port USB	Vert fixe lorsque le périphérique USB connecté est opérationnel. Clignote en vert en cas de panne ou de périphérique non pris en charge.
WPS	Vert fixe lorsque le WPS est opérationnel. Une lumière verte qui clignote lentement indique que la configuration est en cours. Le clignotement rapide du voyant signifie qu'une erreur de configuration est survenue.

Panneau avant (modèles SRP540)

Façade du modèle SRP541W

Panneau avant SRP546W / SRP547W

Voyants de la façade

Le tableau suivant décrit les voyants situés sur le panneau avant des modèles SRP540. Ces voyants permettent de surveiller l'activité du système.

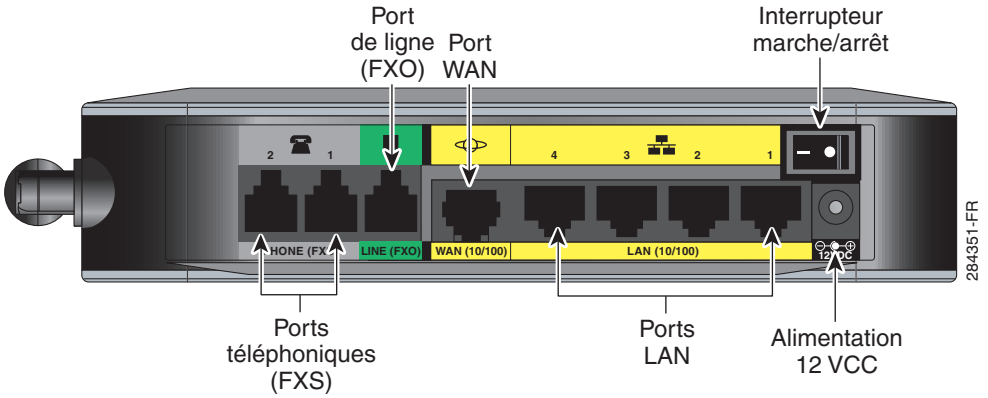
Voyants du panneau avant des modèles SRP540

Lumières	Description
POWER/SYS	Vert fixe lorsque le SRP a démarré et qu'il est prêt à être utilisé. Clignote en vert pendant le démarrage.
Ports LAN (1–4)	Vert fixe lorsqu'une liaison est établie. Clignote en vert en présence d'activité sur le port LAN.
Ports WAN	Vert fixe lorsqu'une liaison Ethernet est établie. Clignote en vert en présence d'activité sur le port WAN.
Port de ligne	Vert fixe lorsque le port est connecté à une ligne RTPC et que le SRP peut émettre et recevoir des appels. Clignote en vert lorsqu'il y a un appel en cours sur le port.
Ports téléphoniques (FXS) (1–4)	Vert fixe lorsque le port est connecté à un téléphone ou un télécopieur et que le SRP est en mesure d'effectuer et de recevoir des appels. Clignote en vert lorsqu'il y a un appel en cours sur le port.
DSL CD (SRP546W/547W uniquement)	Clignote en vert lorsqu'un service DSL est détecté. Vert fixe une fois la synchronisation effectuée.
DSL Data (SRP546W/547W uniquement)	Clignote en vert en présence d'activité DSL sur la ligne.
WLAN	Vert fixe lorsque la radio est sous tension et opérationnelle. Clignote en vert en présence d'activité sans fil sur le port WLAN.
Ports USB (1–2)	Vert fixe lorsque le périphérique USB connecté est opérationnel. Clignote en vert en cas de panne ou de périphérique non pris en charge.
Bouton WPS	Vert fixe lorsque le WPS est opérationnel. Une lumière verte qui clignote lentement indique que la configuration est en cours. Le clignotement rapide du voyant signifie qu'une erreur de configuration est survenue. Pour configurer automatiquement la sécurité sans fil des appareils prenant en charge WPS, maintenez ce bouton enfoncé jusqu'à ce que le voyant du mode WPS clignote. Assurez-vous que le périphérique est situé à proximité de la SRP au moment de la configuration.

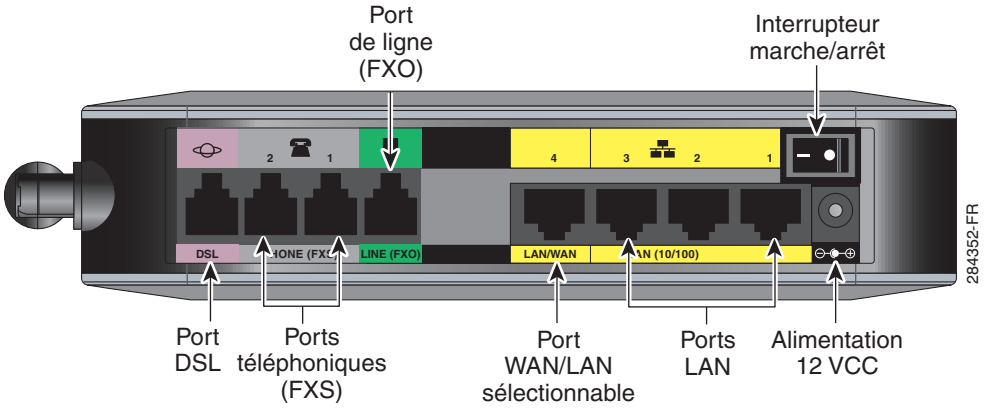
Panneau arrière (modèles SRP520-U)

Les périphériques réseau sont connectés au panneau arrière du SRP. Les ports situés sur le panneau peuvent varier en fonction du modèle.

Panneau arrière SRP521W-U



Panneau arrière SRP526W-U et SRP527W-U

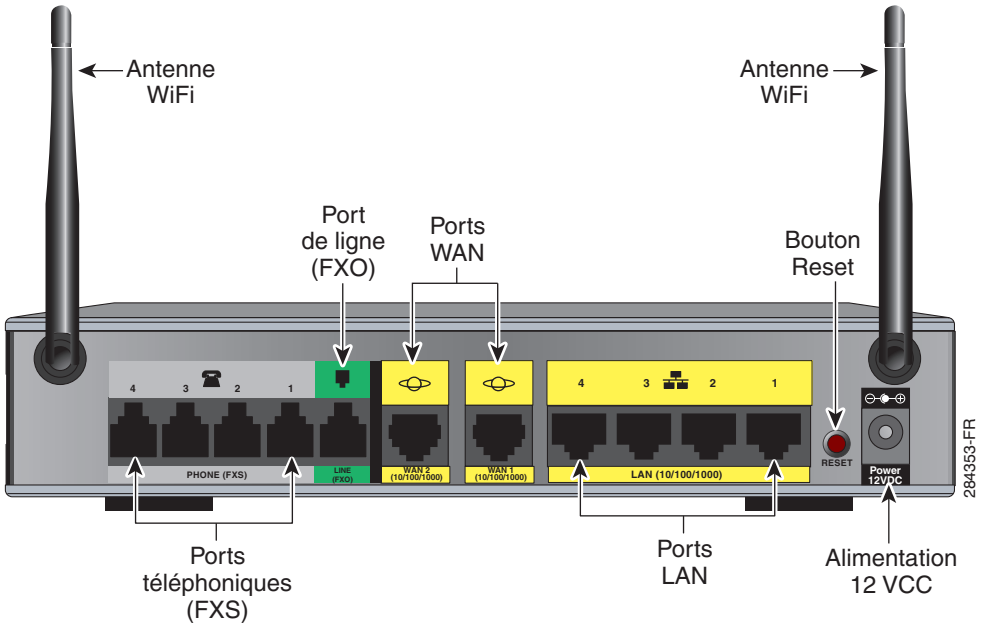


Description du panneau arrière - SRP520-U

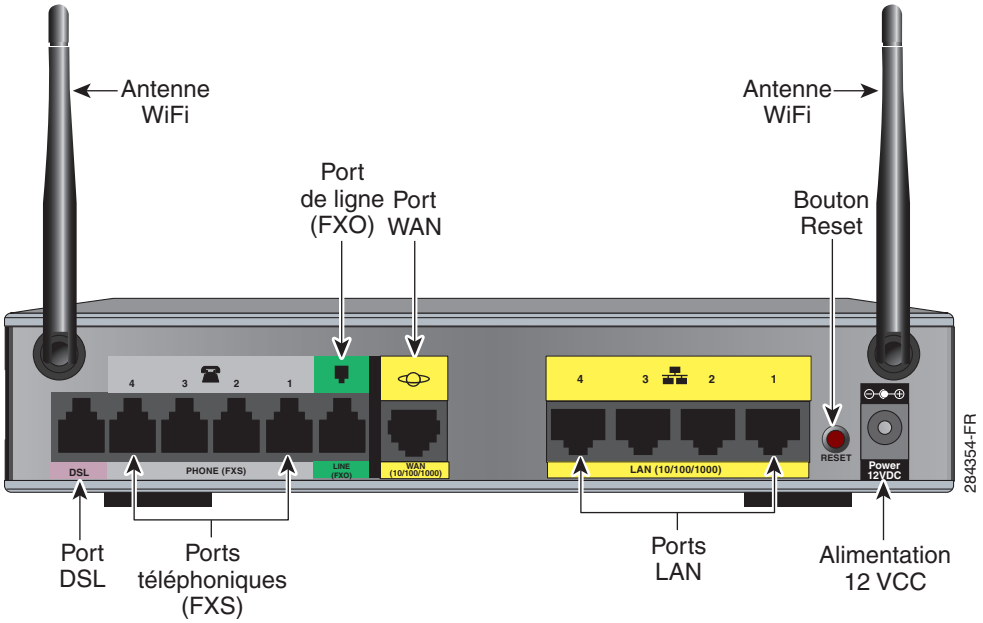
Fonctionnalité	Description
Port DSL SRP526W-U/SRP527W-U uniquement	Établissez une connexion DSL.
Ports téléphoniques (FXS) (1–2)	Permettent de raccorder directement l'unité à un téléphone analogique, un télécopieur ou un périphérique similaire. Si votre téléphone analogique nécessite une ligne distincte, vous devrez peut-être connecter un adaptateur de sonnerie entre le SRP et votre téléphone de sorte que le téléphone sonne lorsqu'il reçoit des appels.
Port de ligne (FXO)	Connectez-vous à une ligne de téléphone analogique.
Port WAN (10/100) SRP521W-U uniquement	Établissez une connexion Internet haut débit Ethernet.
Ports LAN (10/100) (1–4)	Se connecte à un ordinateur câblé et à d'autres périphériques réseau.
WAN/LAN sélectionnable Port (10/100) SRP526W-U/SRP527W-U uniquement	Le port peut être utilisé comme port Ethernet WAN si l'interface ADSL est désactivée. Par défaut, le port ADSL est activé, ce qui permet l'utilisation de ce port pour la connectivité LAN. Pour plus d'informations, reportez-vous au Guide d'administration SRP500.
Interrupteur marche/arrêt	Permet de mettre la SRP sous ou hors tension.
Alimentation 12V CC	Se branche à l'adaptateur d'alimentation fourni.

Panneau arrière (modèles SRP540)

Panneau arrière du modèle SRP541W



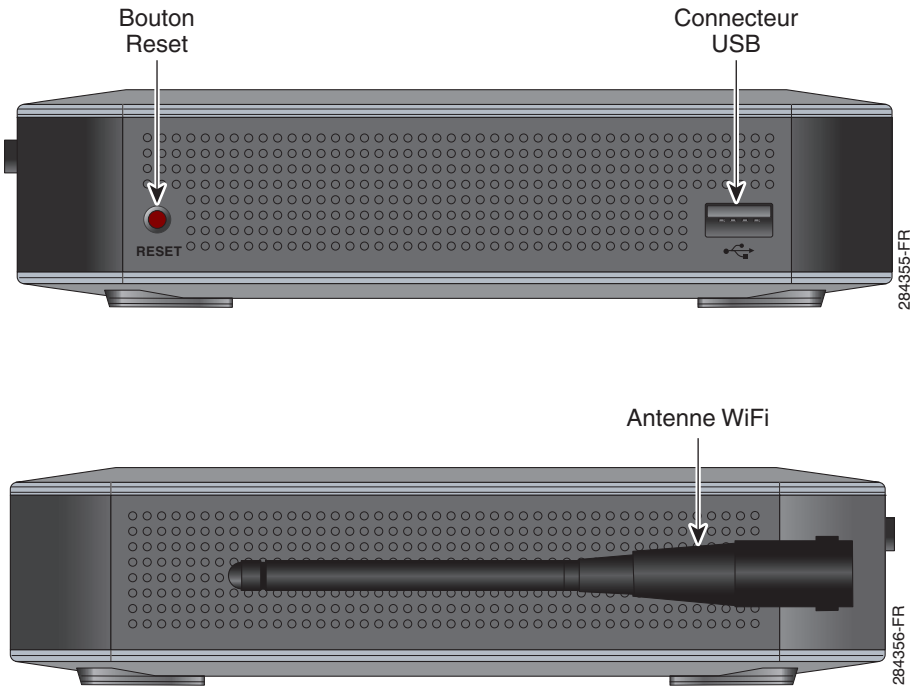
Panneau arrière SRP546W et SRP547W



Descriptions du panneau arrière - SRP540

Fonctionnalité	Description
Port DSL SRP546W/SRP547W uniquement	Établissez une connexion DSL.
Ports téléphoniques (FXS) (1–4)	Permettent de raccorder directement l'unité à un téléphone analogique, un télécopieur ou un périphérique similaire. Si votre téléphone analogique nécessite une ligne distincte, vous devrez peut-être connecter un adaptateur de sonnerie entre le SRP et votre téléphone de sorte que le téléphone sonne lorsqu'il reçoit des appels.
Port de ligne (FXO)	Connectez-vous à une ligne de téléphone analogique.
Port(s) WAN (10/100/1000) Remarque : Le SRP541W a 2 ports WAN.	Établissez une connexion Internet haut débit Ethernet.
Ports LAN (10/100/1000) (1–4)	Se connecte à un ordinateur câblé et à d'autres périphériques réseau.
Bouton Reset	Appuyez sur ce bouton et maintenez-le enfoncé pendant cinq secondes pour réinitialiser la SRP. Appuyez sur ce bouton et maintenez-le enfoncé pendant dix secondes pour rétablir les paramètres d'usine de la SRP. Pour enfoncer le bouton, insérez un trombone ou tout autre objet similaire dans l'ouverture. **ATTENTION** Cela permettra de restaurer les valeurs par défaut du périphérique.
Alimentation 12 VCC	Se branche à l'adaptateur d'alimentation fourni.
Antennes WiFi	Deux antennes WiFi détachables avec connecteurs TNC.

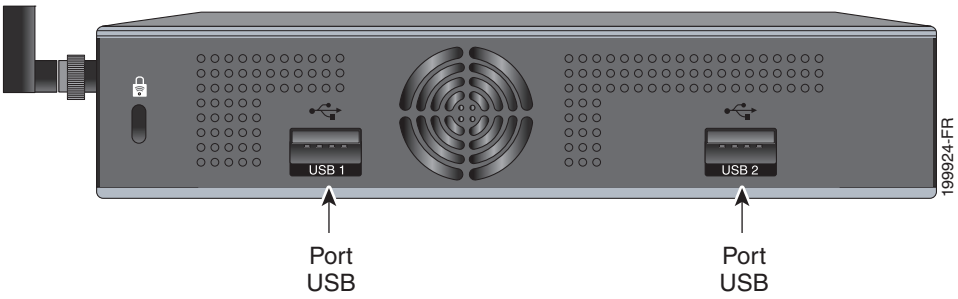
Vue latérale (modèles SRP520-U)



Vue latérale SRP520-U

Fonctionnalité	Description
Bouton Reset	Appuyez sur ce bouton et maintenez-le enfoncé pendant cinq secondes pour réinitialiser la SRP. Appuyez sur ce bouton et maintenez-le enfoncé pendant dix secondes pour rétablir les paramètres par défaut de la SRP. Pour enfoncer le bouton, insérez un trombone ou tout autre objet similaire dans l'ouverture. AVERTISSEMENT Cela aura pour effet de restaurer les valeurs par défaut du périphérique.
Port USB	Permet de raccorder l'unité à un modem USB compatible. Pour de plus amples informations sur la connexion du SRP à un modem USB, voir aussi le chapitre Page Mobile Network, page 46.
Antennes WiFi	Antenne WiFi réglable.

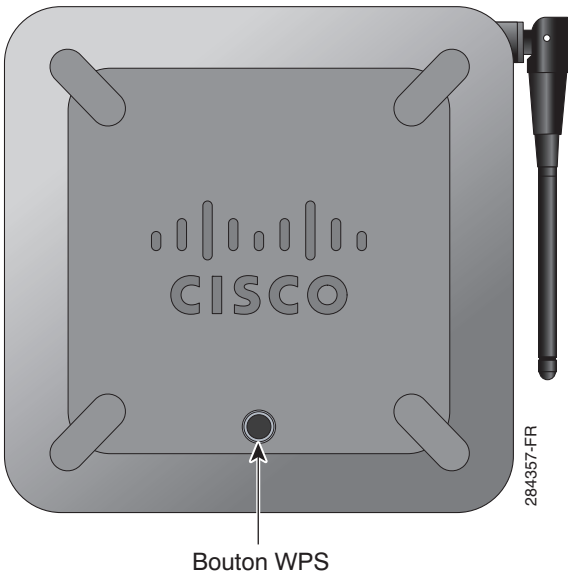
Vue latérale (modèles SRP540)



Vue latérale SRP540

Fonctionnalité	Description
Ports USB (1–2)	Permet de raccorder l'unité aux modems USB compatibles. Pour de plus amples informations sur la connexion du SRP à un modem USB, voir aussi le chapitre **Page Mobile Network, page 46**.

Vue du dessus (modèles SRP520-U)



Vue latérale SRP520-U

Fonctionnalité	Description
Bouton WPS	S'utilise pour configurer automatiquement la sécurité sans fil des périphériques prenant en charge le protocole WiFi Protected Setup (WPS). Pour configurer la fonction WPS, appuyez sur ce bouton et maintenez-le enfoncé jusqu'à ce que le voyant WPS clignote. Assurez-vous que le périphérique est situé à proximité de la SRP au moment de la configuration.

Paramètres par défaut

Le tableau suivant répertorie les paramètres par défaut pour les plates-formes prêtes pour les services.

Paramètres SRP par défaut

Paramètres	Valeur
Device IP	192.168.15.1
Customer username	cisco
Customer password	cisco
Administrator username	admin
Administrator password	admin
DHCP Range	192.168.15.100 à 149
Data VLAN	VLAN 1 : accès aux données par défaut. Par défaut, le masque de sous-réseau IP attribué est 192.168.15.1/24.
Voice VLAN	VLAN 100 : Signalé aux téléphones Cisco VoIP via CDP. Par défaut, le VLAN vocal reçoit le sous-réseau IP 192.168.100.100 à 149.

2

Mise en route à l'aide de l'utilitaire de configuration

Ce chapitre décrit l'utilisation de l'utilitaire de configuration pour les plates-formes prêtes pour les services. Il s'agit d'un utilitaire Web que vous pouvez utiliser pour gérer et configurer votre plate-forme prête pour les services (SRP).

Ce chapitre comprend les sections suivantes :

- **Connexion à l'utilitaire de configuration**
- **Présentation de l'interface de l'utilitaire de configuration**

Connexion à l'utilitaire de configuration

Pour vous connecter à l'utilitaire de configuration des plates-formes prêtes pour les services :

ÉTAPE 1 Configurez votre ordinateur afin qu'il utilise le protocole DHCP pour sa connexion LAN.

Au moyen d'un câble Ethernet, connectez-le à un port LAN disponible (1-4) de la SRP. Votre ordinateur obtiendra automatiquement une adresse IP dans la plage 192.168.15.x.

ÉTAPE 2 Ouvrez un navigateur Web. Dans la barre d'adresse, entrez l'adresse IP par défaut : **http://192.168.15.1**

ÉTAPE 3 Lorsque la fenêtre de connexion s'affiche, saisissez le nom d'utilisateur et le mot de passe par défaut pour vous connecter en tant qu'administrateur.

Le nom d'utilisateur par défaut est **admin**.
Le mot de passe par défaut est **admin**.

REMARQUE Le nom d'utilisateur et le mot de passe respectent la casse.

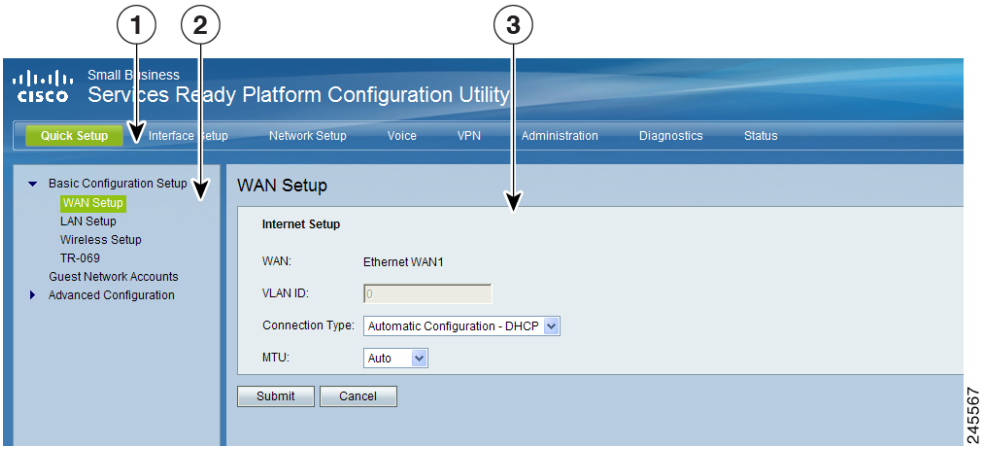
Une fois que vous êtes connecté, l'utilitaire de configuration s'ouvre.

ÉTAPE 4 Poursuivez la configuration de votre SRP à partir des pages de configuration rapide. Reportez-vous au **Le menu Quick Setup, page 29**

Présentation de l'interface de l'utilitaire de configuration

Cette section décrit les zones de la barre du menu principal et les icônes utilisées par l'utilitaire de configuration.

Barre de menu principal



Numéro	Composant	Description
1	Barre de menu	Contient les principales catégories de fonctions. Cliquez sur un élément de menu pour passer à une autre catégorie.
2	Volet de navigation	Permet une navigation facile grâce aux fonctionnalités configurables. Vous pouvez développer les branches principales pour afficher les fonctionnalités secondaires. Cliquez sur le triangle situé en regard du titre de la branche principale pour développer ou réduire son contenu. Cliquez sur le titre d'une fonctionnalité ou d'une fonctionnalité secondaire pour l'ouvrir.
3	Contenu principal	Le contenu principal de la fonctionnalité apparaît dans cette zone.

Icônes

L'utilitaire de configuration dispose d'icônes et de boutons pour les options de configuration les plus utilisées ; voir ci-dessous.

Icône	Description
Icône Edit	Permet de modifier un élément d'une liste.
Icône Add Item	Permet d'ajouter un élément à une liste.
Icône Delete Item	Permet de supprimer un élément d'une liste.
Icônes Increment et Decrement	Permettent de modifier les valeurs numériques. ▪ Cliquez sur l'icône « + » pour incrémenter une valeur. ▪ Cliquez sur l'icône « - » pour réduire une valeur.

3

Le menu Quick Setup

Ce chapitre décrit l'utilisation du menu Quick Setup pour configurer les fonctionnalités de connectivité essentielles et les comptes invité de vos plates-formes prêtes pour les services. Il comprend les sections suivantes :

- **Installation de la configuration de base**
- **Comptes invité au réseau**
- **Configuration avancée**

Le menu Quick Setup est affiché par défaut lorsque vous vous connectez au SRP pour la première fois. Vous pouvez utiliser ces pages de configuration pour mettre rapidement le périphérique en service. Le menu fournit également des liens pratiques vers les fonctions disponibles dans l'utilitaire de configuration.

Installation de la configuration de base

Utilisez la configuration de base pour définir les paramètres WAN, LAN, sans fil et de mise en service à distance pour votre SRP. Pour accéder à ces pages, cliquez sur **Quick Setup > Basic Configuration Setup** dans la barre de menu de l'utilitaire de configuration.

Configuration WAN (Ethernet)

Utilisez la page WAN Setup pour configurer votre interface WAN Ethernet.

ÉTAPE 1 Cliquez sur **Quick Setup > Basic Configuration Setup > WAN Setup**. La fenêtre WAN Setup s'ouvre.

ÉTAPE 2 Sélectionnez le type de connexion selon les exigences de votre fournisseur de services Internet (ISP).

ÉTAPE 3 Spécifiez les paramètres de type de connexion comme indiqué au chapitre **Paramètres de l'interface WAN Ethernet, page 39.**

ÉTAPE 4 Cliquez sur **Submit** pour enregistrer les modifications.

Configuration WAN (ADSL)

Utilisez la page WAN Setup pour configurer rapidement votre interface WAN ADSL.

ÉTAPE 1 Cliquez sur **Quick Setup > Basic Configuration Setup > WAN Setup**. La fenêtre WAN Setup/VC and IP Settings s'ouvre.

ÉTAPE 2 Entrez les paramètres VC (Virtual Connection, connexion virtuelle) et IP comme indiqué au chapitre **Page Internet Setup, page 35.**

ÉTAPE 3 Cliquez sur **Submit** pour enregistrer les modifications.

Configuration LAN

Utilisez la page LAN Setup pour configurer rapidement votre interface LAN.

REMARQUE La configuration rapide suppose que vous allez configurer le SRP de façon à agir en tant que serveur DHCP pour le sous-réseau local principal. Si vous avez besoin de configurations alternatives, accédez à l'ensemble des fonctionnalités via le menu Interfaces.

ÉTAPE 1 Cliquez sur **Quick Setup > Basic Configuration Setup** > **LAN Setup**. La fenêtre LAN Setup s'ouvre.

Cette page affiche le serveur DHCP (LAN par défaut) et les paramètres vocaux. La valeur par défaut est DHCPRule_1 (LAN par défaut) et DHCPRule_voice.

ÉTAPE 2 Si nécessaire, vous pouvez afficher, modifier ou ajouter une entrée DHCP. Pour obtenir plus d'informations, reportez-vous à la section **Page DHCP Server, page 54**.

ÉTAPE 3 Cliquez sur **Submit** pour enregistrer les paramètres.

Configuration sans fil

Utilisez la page Wireless Setup pour configurer rapidement le réseau sans fil.

ÉTAPE 1 Cliquez sur **Quick Setup > Basic Configuration Setup** > **Wireless Setup**. La fenêtre Wireless Setup s'ouvre.

ÉTAPE 2 Spécifiez les paramètres réseau sans fil comme indiqué dans le chapitre **Page Basic Wireless Settings, page 65.**

ÉTAPE 3 Cliquez sur **Submit** pour enregistrer les modifications.

TR-069 (mise en service à distance)

Utilisez la page TR-069 pour configurer la communication avec un serveur de configuration automatique (ACS) via le protocole de gestion WAN CPE TR-069 (CWMP).

ÉTAPE 1 Cliquez sur **Quick Setup > Basic Configuration Setup** > **TR-069**. La fenêtre TR-069 s'ouvre.

ÉTAPE 2 Cliquez sur **Enabled** pour activer la mise en service à distance. Cette option est désactivée par défaut.

ÉTAPE 3 Spécifiez les paramètres de mise en service à distance comme indiqué dans le chapitre **Page TR-069, page 246**.

ÉTAPE 4 Cliquez sur **Submit** pour enregistrer les paramètres.

Comptes invité au réseau

Utilisez la page de réseau invité pour ajouter des comptes invité à votre réseau.

ÉTAPE 1 Cliquez sur **Quick Setup > Guest Network Accounts.** La fenêtre Guest Network Accounts s'ouvre.

ÉTAPE 2 Spécifiez les paramètres de comptes invité comme indiqué dans le chapitre **Page User Account, page 117.**

ÉTAPE 3 Cliquez sur **Submit** pour enregistrer les paramètres.

Configuration avancée

Utilisez les pages Advanced Configuration pour configurer les paramètres avancés pour la voix, la configuration du réseau mobile, le pare-feu, le NAT et la redirection d'une plage de ports.

Pour accéder à ces pages, cliquez sur **Quick Setup > Advanced Configuration Setup** dans l'utilitaire de configuration.

Voix

Utilisez l'option Voice pour gérer et afficher les services et paramètres vocaux. Voir aussi **Configuration de la voix, à la page 122**.

Configuration de réseau mobile

Utilisez l'option Mobile Network Setup pour configurer les paramètres de réseau mobile. Voir aussi **Page Mobile Network, à la page 46**.

Pare-feu

Utilisez l'option Firewall pour configurer les paramètres des filtres de pare-feu. Voir aussi **Firewall, à la page 99.**

NAT

Utilisez l'option NAT pour configurer les paramètres de NAT (Network Address Translation, traduction d'adresses réseau). Voir aussi **Traduction d'adresses de réseau (NAT), à la page 85**.

Redirection d'une plage de ports

Utilisez l'option Port Range Forwarding pour transférer le trafic arrivant sur une plage de ports vers les mêmes ports sur le serveur de destination dans le LAN. Voir aussi **Page Port Forwarding, page 88**.

4

Configuration des interfaces des plates-formes prêtes pour les services

Ce chapitre décrit la configuration des interfaces pour votre SRP. Il comprend les sections suivantes :

- **Configuration des interfaces WAN**
- **Configuration des interfaces VLAN et des ports LAN**
- **Configuration d'un LAN sans fil**
- **Utilisation de l'interface de gestion**

Pour accéder à ces pages, cliquez sur **Interface Setup** dans la barre de menu de l'utilitaire de configuration.

Configuration des interfaces WAN

Cette section comprend les rubriques suivantes :

- **Page Internet Setup**
- **Page Internet Option**
- **Page Mobile Network**
- **Page Multi-WAN Configuration**

Pour accéder à ces pages, cliquez sur **Interface Setup > WAN** à partir de l'utilitaire de configuration.

Page Internet Setup

La page Internet Setup permet de configurer les paramètres de mise en réseau WAN.

REMARQUE Une fois que vous avez configuré les paramètres d'interface, nous vous recommandons de créer un nouveau mot de passe pour votre SRP. Pour le modifier, consultez la section **Page User List, page 256**. Cette précaution permet de renforcer la sécurité en protégeant la SRP contre toute modification non autorisée.

ÉTAPE 1 Cliquez sur **Interface Setup > WAN > Internet Setup**. La fenêtre Internet Setup s'ouvre. La liste des interfaces WAN contient la valeur par défaut du système et la route des communications vocales par défaut, le type d'interface, le type de connexion Internet, ainsi que l'adresse IP et le masque de sous-réseau de chaque interface.

ÉTAPE 2 Configurez les interfaces.

a. Dans la colonne Interface, cliquez sur l'interface à configurer.

b. Configurez les paramètres des interfaces physiques. Deux séries d'options sont disponibles, une pour DSL et l'autre pour Ethernet.

- Pour une interface DSL, choisissez un type de modulation dans la liste déroulante. La valeur par défaut est MultiMode (recommandée), qui détecte automatiquement le type de modulation de la ligne.
- Pour une interface Ethernet, sélectionnez le paramètre de contrôle de flux (activé par défaut), la vitesse d'interface (la valeur par défaut est Auto-negotiate) ou remplacez l'adresse MAC utilisée par l'interface. Pour utiliser l'adresse MAC de l'ordinateur utilisé pour configurer la SRP, cliquez sur le bouton **Clone Your PC's MAC**.

c. Lorsque vous avez terminé, cliquez sur **Submit**.

ÉTAPE 3 Configurez l'adressage d'interface.

a. Dans la liste des interfaces WAN, sélectionnez un PVC DSL ou une sous-interface Ethernet selon votre modèle.

- Pour configurer une interface PVC DSL, cliquez sur l'icône en forme de stylet **Edit** en regard de l'interface PVC0. Les paramètres Internet Setup de la fenêtre PVC0 interface s'affichent.

  Spécifiez les paramètres Internet Setup comme indiqué dans le tableau **Paramètres Virtual Channel (VC).** Le type d'encapsulation que vous choisissez peut modifier les autres options figurant dans cette page. Pour obtenir plus d'informations, reportez-vous à la section **Paramètres d'encapsulation, page 41.**

- Pour configurer une sous-interface Ethernet, cliquez sur l'icône en forme de stylet **Edit** en regard de l'interface WAN. Entrez les paramètres comme indiqué à la section **Ajout d'une sous-interface, page 38.**

b. Cliquez sur **Submit** pour enregistrer les modifications.

ÉTAPE 4 Dans la liste déroulante, sélectionnez la route par défaut pour l'interface que vous configurez.

REMARQUE Cette route par défaut de l'interface sert à sélectionner l'interface logique sortante lorsque le basculement comporte des commutateurs entre les interfaces physiques.

ÉTAPE 5 Pour afficher les informations d'interface, sélectionnez une interface dans la liste WAN Interface Detail. Cette liste affiche les informations relatives à l'interface sélectionnée, comme il est décrit dans le tableau **Paramètres de WAN Interface Detail**.

Paramètres Virtual Channel (VC)

Encapsulation	Protocole utilisé entre votre passerelle haut débit et les serveurs de votre ISP. La plupart des encapsulations sont définies dans les normes Internet appelées Requests For Comments (RFC). Deux de ces encapsulations sont dérivées du protocole point à point (PPP) : PPP over Ethernet (PPPoE) et PPP over ATM (PPPoA). Les options disponibles sont IPoA, PPPoE, PPPoA, et l'encapsulation EoA RFC 1483 Bridged.
Multiplexing	Sélectionnez la méthode utilisée pour acheminer différents types de données via différents circuits virtuels (VC) sur le réseau ATM. Vous pouvez choisir l'une des options suivantes : ▪ Logical Link Control (LLC) encapsulation (également appelé LLC-SNAP). Il s'agit du paramètre par défaut. ▪ Virtual Channel (VC) multiplexing (également appelé VC-Mux).

Paramètres Virtual Channel (VC)

QoS Type	Méthode Quality of Service (QoS) DSL que votre ISP utilise sur votre ligne : UBR (Unspecified Bit Rate), CBR (Constant Bit Rate), RTVBR (Real-Time Variable Bit Rate) ou NRTVBR (Non-Real-Time Variable Bit Rate). CBR offre la meilleure garantie en matière de faible latence. UBR n'en offre aucune, mais cette option est généralement utilisée pour la plupart des services de données haut débit. ▪ **Pcr Rate** : Lorsque la QoS est définie sur CBR, VBR_RT ou VBR_NRT, entrez ici le débit maximal des cellules (PCR) dans les cellules par seconde. ▪ **Scr Rate** : Lorsque la QoS est définie sur VBR_NRT ou VBR_RT, entrez ici le taux de cellules admissibles (SCR) dans les cellules par seconde. ▪ **MBS** : Lorsque la QoS est définie sur VBR_NRT ou VBR_RT, entrez ici les MBS dans les cellules par seconde. ▪ **CDVT** : Lorsque la QoS est définie sur CBR, VBR_NRT ou VBR_RT, entrez ici les CDVT dans les cellules par seconde.
VPI/VCI Auto Detect	Active ou désactive la détection automatique des valeurs VPI et VCI qui servent à l'identification de votre ligne par le réseau ATM. Les valeurs VPI (Virtual Path Identifier) et VCI (Virtual Channel Identifier) sont utilisées pour l'identification de votre ligne par le réseau ATM de votre ISP. La SRP détecte automatiquement les services DSL vérifiés sur les paires VC suivantes : 0/35, 8/35, 0/43, 0/51, 0/59, 8/43, 8/51, 8/59, 0/38.

Paramètres de WAN Interface Detail

Physical and Logical Link Status	État de l'interface physique : connecté ou déconnecté. Ce champ ne reflète pas l'état du protocole (Ethernet, PPP, etc.) qui s'exécute sur l'interface.
IP Address	Adresse IP affectée à l'interface.
Netmask	Masque de sous-réseau.
Gateway	Adresse IP du serveur ISP.
Host Name	Nom d'hôte, le cas échéant.

Paramètres de WAN Interface Detail

Domain Name	Nom de domaine, le cas échéant.
MTU Type	Auto ou Custom.
MTU Size	Taille de MTU actuelle. Ce paramètre s'affiche même si « Auto » est sélectionné.
DNS 1,2,3	Adresses IP des serveurs DNS si elles sont configurées.
Static DNS Servers 1, 2, 3	Adresses IP des serveurs DNS statiques si elles sont configurées.
Encapsulation VLAN	Si ce paramètre est activé, un en-tête IEEE 802.1q VLAN est ajouté au trafic sortant pour un PVC ADSL, ce qui permet à certains prestataires de services de contrôler la qualité de service en fonction des valeurs prioritaires IEEE 802.1p associées.
VLAN ID	ID VLAN utilisé si l'encapsulation VLAN est activée.

Ajout d'une sous-interface

Utilisez la liste des interfaces WAN de la fenêtre Internet Setup pour ajouter une sous-interface à la SRP. Ces options sont identiques à celles qui sont disponibles pour configurer une interface WAN principale, sauf que vous pouvez configurer une sous-interface Ethernet pour PPTP ou L2TP.

La SRP prend en charge plusieurs interfaces logiques par port physique. Pour les interfaces ADSL, vous pouvez configurer jusqu'à 4 interfaces PVC. Pour les ports Ethernet, les interfaces VLAN sont créées en tant que partie intégrante d'une liaison IEEE 802.1p.

Sous-interface Ethernet

La SRP prend également en charge les VLAN qui peuvent être utilisés en tant que VLAN locaux ou sous-interfaces WAN. Les modèles SRP520 prennent en charge jusqu'à 5 connexions VLAN. Les modèles SRP540 prennent en charge jusqu'à 10 connexions VLAN.

ÉTAPE 1 Pour ajouter une nouvelle connexion Internet logique, sélectionnez le WAN de niveau supérieur dans la page Internet Setup et cliquez sur l'icône sous forme de page **Add**. La fenêtre Internet Setup s'ouvre pour la nouvelle connexion Internet.

ÉTAPE 2 Sélectionnez le type de connexion requis par votre ISP, comme indiqué dans le tableau **Paramètres de l'interface WAN Ethernet** ci-dessous.

ÉTAPE 3 Choisissez une option MTU dans la liste déroulante. Sauf modification demandée par votre ISP, nous vous recommandons de définir la méthode MTU sur **Auto**, ce qui permet au périphérique de choisir automatiquement la taille. La taille par défaut est 1 500 octets.

Pour spécifier une autre taille MTU, choisissez **Manual** dans la liste déroulante et saisissez la taille en octets. La taille standard pour les réseaux Ethernet est 1 500 octets. Pour les connexions PPPoE, la valeur type est 1 492 octets.

ÉTAPE 4 Cliquez sur **Submit** pour enregistrer les modifications. La nouvelle connexion est ajoutée à la liste des interfaces WAN dans la page Internet Setup.

Paramètres de l'interface WAN Ethernet

WAN	Nom de l'interface physique : WAN1 Ethernet ou WAN2 Ethernet (SRP540 uniquement).
VLAN ID	Saisissez l'ID VLAN de la nouvelle sous-interface logique. Notez que la première interface logique d'un port Ethernet reçoit l'ID VLAN 0 (aucune balise VLAN). Cela n'est pas modifiable.
Connection Type	Type de connexion Internet fourni par votre ISP.
	Automatic Configuration/DCHP Type de connexion souvent utilisé avec les modems câble. Choisissez cette option si votre ISP n'a affecté aucune adresse IP statique à votre compte et a utilisé à la place le protocole DHCP (Dynamic Host Control Protocol) pour affecter une adresse IP dynamiquement. Aucune autre information n'est requise pour cette sélection.
	Static IP Choisissez cette option si votre ISP vous fournit une adresse IP statique (permanente). Renseignez les champs **Internet IP Address** et **Subnet Mask** et entrez une adresse IP dans le champ **Default Gateway**. Vous pouvez aussi saisir les adresses IP de trois serveurs de système de noms de domaine (DNS) au plus.

Paramètres de l'interface WAN Ethernet

	PPPoE Choisissez cette option si votre ISP utilise le protocole PPPoE (Point-to-Point Protocol over Ethernet). Saisissez le nom d'utilisateur dans le champ **Username** et le mot de passe dans le champ **Password** pour votre compte ISP, ainsi que le nom du service dans **Service Name** s'il est requis par votre ISP. Sélectionnez l'option **Connect on Demand** ou **Keep Alive**. **Connect on Demand** Ouvre une connexion uniquement lorsque l'utilisateur tente de se connecter au réseau Internet. La connexion prend fin automatiquement si une période d'inactivité dépasse le délai d'inactivité maximal spécifié (en minutes). Nous vous recommandons cette option si vous êtes facturé en fonction de votre durée de connexion. Les ordinateurs envoient souvent des informations au réseau Internet si la messagerie ou un navigateur Web n'est pas utilisé. Cela peut prolonger la durée de session. **Keep Alive** Cette option permet de garder votre connexion active indéfiniment, même si elle est inactive dans les faits.
	PPTP Sélectionnez cette option si votre ISP utilise le protocole de tunnellisation point à point (PPTP). Indiquez l'adresse de votre compte dans le champ **PPTP Server IP**, le nom d'utilisateur de votre compte dans le champ **Username** et le mot de passe de votre compte dans le champ **Password**. Si votre prestataire de services n'affecte aucune adresse IP dynamiquement, désactivez DHCP et indiquez les informations fournies pour votre compte dans les champs **Internet IP address**, **Subnet Mask** et **Gateway**. Sélectionnez l'option **Connect on Demand** ou **Keep Alive**.

Paramètres de l'interface WAN Ethernet

	L2TP Sélectionnez cette option si votre ISP utilise L2TP (Layer 2 Tunneling Protocol). Indiquez l'adresse de votre compte dans le champ L2TP Server IP, le nom d'utilisateur de votre compte dans le champ Username et le mot de passe de votre compte dans le champ Password. Si votre prestataire de services n'affecte aucune adresse IP dynamiquement, désactivez **DHCP** et indiquez les informations fournies pour votre compte dans les champs **Internet IP address**, **Subnet Mask** et **Gateway**. Sélectionnez l'option **Connect on Demand** ou **Keep Alive**.
MTU (Maximum Transmission Unit ou unité de transmission maximale)	Taille en octets du plus grand paquet qui peut être envoyé via le réseau. Cette valeur est généralement égale à 1 500 octets, mais il peut être nécessaire de la réduire pour certains services haut débit. Consultez votre prestataire de services pour connaître les besoins spécifiques.
DNS 1-3	(Facultatif) Entrez les adresses IP de trois serveurs DNS au maximum ou laissez les champs vides pour permettre à un serveur DNS d'être affecté dynamiquement. Cette option ne peut pas être configurée pour une sous-interface WAN.

Paramètres d'encapsulation

Cette section décrit les paramètres d'encapsulation ADSL que vous pouvez choisir dans les paramètres VC de la page Internet Setup. Les options disponibles sont IPoA, PPPoE, PPPoA, et l'encapsulation EoA RFC 1483 Bridged.

L'encapsulation est le protocole utilisé entre la SRP et les serveurs de votre ISP. La plupart des encapsulations sont définies dans les normes Internet appelées Requests For Comments (RFC). Deux de ces encapsulations sont dérivées du protocole point à point (PPP) : PPP over Ethernet (PPPoE) et PPP over ATM (PPPoA).

Paramètres IPoA

Choisissez IPoA pour autoriser l'encapsulation directe du trafic IP sur le circuit virtuel ATM DSL. Entrez les informations requises, telles qu'elles vous sont fournies par votre ISP : adresse IP Internet, masque de sous-réseau et adresse IP de la passerelle par défaut. Vous pouvez aussi indiquer les adresses IP du serveur DNS principal et du serveur DNS auxiliaire.

Paramètres IPoA

Internet IP Address and Subnet Mask	Adresse IP et masque de sous-réseau de la SRP tels qu'ils apparaissent aux utilisateurs externes sur le réseau Internet (notamment votre ISP). Votre ISP vous fournira ces informations.
Default Gateway	Votre ISP vous fournira l'adresse IP de la passerelle.
Primary/ Secondary DNS	Permet de définir un ou deux serveurs DNS. La SRP utilise ces informations pour résoudre les noms de domaine pour les fonctionnalités configurées localement et peut également les transmettre aux clients locaux via DHCP.

Paramètres PPPoE

Sélectionnez PPPoE pour exécuter un PPP encapsulé Ethernet sur le circuit virtuel ATM DSL. Saisissez le nom d'utilisateur et le mot de passe fournis par votre ISP. Vous pouvez aussi spécifier le nom du service PPP s'il vous a été fourni par votre prestataire de services.

Paramètres PPPoE

Username and Password	Saisissez les chaînes que votre ISP vous a demandé d'utiliser. Le nom de l'utilisateur peut s'appeler « nom d'utilisateur », « nom de connexion » ou « connexion ».
Service Name	Chaîne requise par certains ISP. Entrez ces informations uniquement si votre ISP le demande.
Connect on Demand	Cliquez sur cette option pour que la passerelle haut débit se connecte à votre ISP lorsqu'une connexion est requise et se déconnecte lorsque la ligne de votre ISP a été inactive pendant une durée déterminée. La connexion et la déconnexion sont automatiques. Vous pouvez également régler le temps d'inactivité maximal. La valeur par défaut est 20 minutes. Vous pouvez choisir Keep Alive au lieu de Connect On Demand (voir ci-dessous). Dans la plupart des cas, vous pouvez choisir l'une ou l'autre option sans consulter votre ISP.
Keep Alive	Cliquez sur cette option pour que la passerelle maintienne constamment le connexion à votre ISP. Si le lien est interrompu pendant un certain nombre de secondes (le « temps devant s'écouler avant rappel »), la passerelle essaie automatiquement de le rétablir. Par défaut, le temps devant s'écouler avant rappel est de 20 secondes.

Paramètres PPPoE

MTU	En général, les informations d'en-tête supplémentaires utilisées pour les connexions PPPoE sur ADSL limitent la taille maximale du paquet qui peut être envoyé à 1 492 octets. Activez ce paramètre uniquement si votre ISP vous le demande.
LCP Echo-Request Interval	(Modèles SRP547W/SRP546W uniquement) Spécifiez une valeur en secondes dans le champ **LCP Echo Interval**. La valeur par défaut est 30 secondes. Cela détermine la fréquence à laquelle la SRP envoie une requête d'écho LCP à intervalles réguliers à l'ISP pour vérifier que la connexion PPPoE est active.

Paramètres PPPoA

Choisissez PPPoA pour exécuter PPP directement sur le circuit virtuel ATM DSL. Entrez le nom d'utilisateur et le mot de passe fournis par votre ISP.

Paramètres PPPoA

Username and Password	Saisissez les chaînes que votre ISP vous a demandé d'utiliser. Le nom de l'utilisateur peut s'appeler « nom d'utilisateur », « nom de connexion » ou « connexion ».
Connect on Demand	Cliquez sur cette option pour que la passerelle haut débit se connecte à votre ISP lorsqu'une connexion est requise et se déconnecte lorsque la ligne de votre ISP a été inactive pendant une durée déterminée. La connexion et la déconnexion sont automatiques. Vous pouvez également modifier le temps d'inactivité maximal. Le paramètre par défaut est égal à 20 minutes. Vous pouvez choisir Keep Alive au lieu de Connect On Demand (voir ci-dessous). Dans la plupart des cas, vous pouvez choisir l'une ou l'autre option sans consulter votre ISP.
Keep Alive	Cliquez sur cette option pour que la passerelle maintienne constamment le connexion à votre ISP. Si le lien est interrompu pendant un certain nombre de secondes (le « temps devant s'écouler avant rappel »), la passerelle essaie automatiquement de le rétablir. Par défaut, le temps devant s'écouler avant rappel est de 20 secondes.

EoA RFC 1483 Bridged

Utilisez cette encapsulation pour ponter le trafic local avec le PVC DSL. Si vous utilisez un service Ethernet sur ATM, vous pouvez choisir de configurer l'adresse IP WAN de manière statique ou dynamique.

Pour ponter le trafic à un périphérique connecté localement (en utilisant la SRP comme modem DSL uniquement pour ce PVC), créez un VLAN comprenant ce PVC et le port LAN Ethernet auquel le périphérique est connecté. Le périphérique local pourra alors mettre fin à la connexion IP (via le protocole PPPoE) directement.

Paramètres EoA RFC 1483 Bridged

IP Settings	Sélectionnez le paramètre IP. La valeur par défaut est Obtain an IP Address Automatically. Si vous avez sélectionné Manual, saisissez l'adresse IP, le masque, la passerelle et les paramètres DNS.

Paramètres d'encapsulation DSL communs

Les paramètres supplémentaires suivants s'affichent lorsque vous sélectionnez un paramètre d'encapsulation DSL. Ces paramètres sont communs à toutes les encapsulations DSL.

Paramètres d'encapsulation DSL

MAC Address Clone	Permet de spécifier les valeurs du paramètre MAC Address Clone. Activez cette fonction si votre ISP vous demande d'enregistrer une adresse MAC pour accéder au réseau Internet. ▪ Pour cloner votre adresse MAC, sélectionnez **Enabled** puis entrez l'adresse MAC enregistrée précédemment. ▪ Si vous avez déjà enregistré une autre adresse MAC et que vous ne souhaitez pas vous enregistrer à nouveau auprès de votre ISP, cliquez sur le bouton **Clone Your PC's MAC.** Cela vous permet d'affecter l'adresse MAC enregistrée précédemment à la SRP.

Paramètres d'encapsulation DSL

802.1Q VLAN Encapsulation	Pour activer l'encapsulation 802.1Q, sélectionnez **Enabled** (la valeur par défaut est Disabled). Entrez ensuite une valeur pour l'ID VLAN Les valeurs sont comprises entre 0 et 4079.
MTU	Choisissez une option MTU dans la liste déroulante. Sauf modification demandée par votre ISP, nous vous recommandons de définir la méthode MTU sur **Auto**. La taille par défaut est 1 500 octets.

Page Internet Option

Si nécessaire, utilisez la page Internet Option pour compléter les informations configurée pour votre connexion Internet.

ÉTAPE 1 Cliquez sur **Interface Setup > WAN > Internet Option**. La fenêtre Internet Option s'ouvre.

ÉTAPE 2 Indiquez une valeur dans les champs **Host Name** et **Domain Name** si elle vous a été fournie par votre ISP.

ÉTAPE 3 Renseignez le champ **IP addresses** pour trois serveurs DNS au maximum.

REMARQUE La SRP permet de spécifier les informations de serveur DNS dans un certain nombre de contextes, ce qui vous permet de répondre à vos besoins spécifiques.

Chaque interface WAN autorise la configuration statique ou dynamique de serveurs spécifiques de connexion primaires, secondaires et tertiaires. Vous pouvez également configurer statiquement les serveurs primaires, secondaire et tertiaires de manière globale.

Pour déterminer les serveurs à utiliser pour la résolution des noms internes, la SRP extrait les trois premières adresses d'une liste qu'elles construit dans l'ordre indiqué ci-dessous.

- Serveurs primaires dans Internet Options, WAN1, WAN2 et 3G.
- Serveurs secondaires dans Internet Options, WAN1, WAN2 et 3G.

Serveurs tertiaires dans Internet Options, WAN1, WAN2 et 3G.

ÉTAPE 4 Activez **Schedule WAN Reconnect** pour que toutes les connexions WAN soient redémarrées à un moment donné. Si cette option est activée, renseignez le champ **Reconnect Time** avec l'heure et la minute.

ÉTAPE 5 Cliquez sur **Submit** pour enregistrer les modifications.

Internet Options

Host Name	Nom d'hôte fourni par votre ISP.
Domain Name	Nom de domaine fourni par votre ISP.
Static DNS 1–3	Renseignez le champ IP addresses pour trois serveurs DNS au maximum.
Scheduled WAN Reconnect	Activez cette option pour que toutes les connexions WAN redémarrent à une heure de reconnexion spécifiée.
Reconnect Time	Si Scheduled WAN Reconnect est activé, définissez l'heure de reconnexion en indiquant l'heure et la minute.

Page Mobile Network

Utilisez la page Mobile Network pour configurer les paramètres de votre réseau mobile. Vous pouvez configurer votre SRP de telle sorte qu'elle se connecte à un modem USB haut débit mobile connecté à son interface USB. Pour obtenir des informations sur les modems compatibles, cliquez sur le lien Technical References à l'adresse suivante :

http://www.cisco.com/go/srp500resources

Lorsqu'un modem USB est connecté à la SRP, il est automatiquement détecté et configuré. Une fois le modem détecté, une configuration personnalisée de l'accès au réseau peut être ajoutée.

- Si la SRP500 est configurée pour la fonction Connection failover, le modem USB tente uniquement de se connecter lorsque les interfaces de priorité supérieure ne se connectent pas.
- Si la fonction Connection Failover n'est pas utilisée, le modem USB tente de se connecter immédiatement.

Le modem USB haut débit mobile est principalement destiné aux services de données. La qualité vocale ne peut être garantie sur le réseau mobile.

ÉTAPE 1 Cliquez sur **Interface Setup > Mobile Network**. La fenêtre Mobile Network s'ouvre.

ÉTAPE 2 Connectez-vous au modem USB. Si la carte est prise en charge par la SRP, elle est détectée automatiquement et s'affiche dans la page Mobile Network.

ÉTAPE 3 Sélectionnez le mode de connexion **Auto** ou **Manual**. Le mode par défaut est Auto.

- Pour que votre modem établisse une connexion automatiquement, sélectionnez **Auto**.

  REMARQUE La fonctionnalité de récupération de connexion Ethernet ne fonctionne que si le mode de connexion est défini sur Auto. Si vous sélectionnez Auto, vous devez également sélectionner **Connect on Demand** ou **Keep Alive**.

- Pour connecter ou déconnecter votre connexion de modem manuellement, sélectionnez le mode **Manual**.

  REMARQUE Si vous ne parvenez pas à établir une connexion, sélectionnez le mode **Manual** , composez le numéro et entrez le nom d'utilisateur et le mot de passe. Pour certains services de données mobiles, il peut être nécessaire de configurer l'APN (Access Point Name), le numéro, le nom d'utilisateur et le mot de passe.

ÉTAPE 4 Vérifiez que le champ Card Status contient l'état de votre carte mobile.

ÉTAPE 5 Au besoin, sélectionnez un protocole de tunnel dans la liste déroulante.

ÉTAPE 6 si nécessaire, modifiez les paramètres de réseau mobile dans la zone **Mobile Network Setup.**

REMARQUE Pour configurer manuellement votre carte de réseau mobile, cliquez sur l'option Manual dans le champ Configure Mode.

ÉTAPE 7 Cliquez sur **Submit** pour enregistrer les paramètres.

Paramètres Mobile Network

Paramètres généraux	
Connect Mode	Choisissez le mode **Auto** ou **Manual**. Pour que votre modem établisse une connexion automatiquement, sélectionnez le mode **Auto**. Si vous utilisez le mode manuel, vous devez accéder à l'utilitaire de configuration pour établir une connexion Internet via la connexion mobile. Cliquez sur **Connect** pour établir une connexion en cas de besoin. Cliquez sur **Disconnect** pour interrompre la connexion. **Connect on Demand** : sélectionnez cette option pour que la SRP mette fin à la connexion Internet lorsqu'elle est inactive pendant une période définie (durée d'inactivité maximale). Si votre connexion Internet a été interrompue en raison d'une inactivité, cette option permet au modem de la rétablir automatiquement dès qu'un utilisateur tente d'accéder à nouveau à Internet. Dans le champ **Max Idle Time**, saisissez le nombre de minutes d'inactivité devant s'écouler avant l'interruption d'une connexion Internet. Le délai d'inactivité maximal par défaut est de 5 minutes. **Keep Alive** : Sélectionnez cette option pour permettre à la SRP de vérifier votre connexion internet à l'intervalle spécifié (temps devant s'écouler avant rappel). Si vous êtes déconnecté, la SRP rétablit automatiquement votre connexion. Dans le champ Redial period, indiquez la fréquence à laquelle la SRP doit vérifier votre connexion Internet. Par défaut, le temps devant s'écouler avant rappel est de 30 secondes.

Paramètres Mobile Network

Tunnel Protocol	Comme avec les ports Ethernet WAN, vous pouvez sélectionner PPTP ou L2TP via le modem USB. Pour plus de détails sur les options, consultez la section **Paramètres de l'interface WAN Ethernet, page 39.** **REMARQUE** Seul l'adressage dynamique est autorisé sur cette interface. **NONE**. Sélectionnez cette option pour désactiver la tunnellisation des protocoles. Il s'agit du paramètre par défaut. **PPTP/L2TP**. Sélectionnez PPTP ou L2TP selon le service à utiliser. Vous devez fournir l'adresse IP du serveur, le nom d'utilisateur et le mot de passe.
Card Status	Affiche l'état actuel de connexion du modem : en cours d'initialisation, en cours de connexion, connecté, en cours de déconnexion ou déconnecté. Les messages ci-dessous peuvent également s'afficher. ▪ Please set APN manually (ce message s'affiche lorsque la SRP ne parvient pas à déterminer l'APN de l'opérateur en mode automatique) ▪ Searching for service... ▪ no SIM card ▪ SIM locked ▪ SIM busy ▪ SIM ready ▪ pin code needed ▪ pincode error ▪ Card is locked ▪ Card is not activated ▪ Card initialized error ▪ erreur Si Connect Mode est défini sur Manual, vous pouvez cliquer sur un bouton pour connecter ou déconnecter votre modem.

Paramètres Mobile Network

Mobile Network Setup	
Configure Mode	La SRP détecte automatiquement les modems pris en charge et présente la liste des configurations par défaut appropriées. Pour remplacer l'un de ces paramètres (excepté le code PIN de la carte SIM), sélectionnez le mode de configuration manuelle.
Card Model	Modèle de carte de données inséré dans le lecteur USB. Les cartes non prises en charge sont signalées comme non reconnues.
Access Point Name (APN)	Réseau Internet auquel le périphérique mobile se connecte. Entrez le nom du point d'accès fourni par votre prestataire de services de réseau mobile. Ce champ ne s'affiche que pour les cartes GSM.
Dial Number	Numéro à composer pour la connexion Internet. Entrez le numéro requis pour votre modem.
Username/ Password	(Facultatif) Dans les champs **Username** et **Password**, indiquez les informations fournies par votre prestataire de services de réseau mobile.
SIM PIN	(Facultatif) Code PIN associé à votre carte SIM. Saisissez le code PIN de votre carte SIM dans ce champ. Ce champ ne s'affiche que pour les cartes GSM.
Server Name	(Facultatif) Nom du serveur de la connexion Internet (s'il a été fourni par votre prestataire de services).
Authentication	Type d'authentification utilisé par votre prestataire de services. Choisissez le type d'authentification dans la liste déroulante. La valeur par défaut est Auto. Si vous ne savez pas quel type d'authentification utiliser, conservez la valeur par défaut.
Service Type	Sélectionnez le type de connexion de services de données mobiles généralement disponible en fonction du signal de service de votre zone. Options disponibles : **HSDPA/3G/ UMTS Preferred**, **HSDPA/3G/UMTS Only** et **GPRS Only**. Si votre emplacement prend en charge un seul service de données mobiles, vous pouvez configurer une connexion améliorée. La première sélection recherche toujours le service HSPDA/3G/UMTS ou bascule automatiquement sur le service GPRS uniquement lorsqu'il est disponible.

Paramètres Mobile Network

LTE Service	Choisissez un service sans fil LTE dans le menu déroulant. Options disponibles : 3G only, 4G only ou Auto. La valeur par défaut est Auto.

Page Multi-WAN Configuration

Une connexion Internet peut être établie via un câble Ethernet (connecté au port WAN), via ADSL (connecté au port ADSL), ou via un modem USB compatible (connecté au port USB). Lorsque vous activez le basculement de la connexion, vous pouvez connecter simultanément ces éléments, mais un seul d'entre eux peut être utilisé à la fois pour établir un lien.

Chaque fois que la connexion Internet échoue sur l'interface utilisée, la SRP tente automatiquement d'activer une autre connexion sur l'autre interface en fonction de la priorité. Chaque fois que la connexion Internet est récupérée sur une interface WAN qui a une priorité supérieure, la SRP tente automatiquement de la rétablir via ce WAN.

Lorsque le basculement de la connexion est désactivé, la SRP tente d'utiliser toutes les interfaces WAN disponibles. Dans ce cas, les protocoles de routage ou le routage basé sur des stratégies sont utilisés pour acheminer le trafic s'ils sont configurés. Sinon, l'ensemble du trafic est acheminé via l'interface dont la priorité est la plus élevée. Le trafic peut aussi être réparti entre les interfaces connectées selon un schéma de pondération prédéfini. En plus du routage basé sur les stratégies, les routes statiques peuvent également être utilisées pour acheminer le trafic.

ÉTAPE 1 Cliquez sur **Interface Setup > Multi-WAN Config**. La fenêtre Multi-WAN Config s'ouvre.

ÉTAPE 2 Pour activer le basculement de la connexion, sélectionnez **Enabled**. Lorsque cette option est activée, la SRP définit l'interface avec la priorité la plus élevée.

REMARQUE Le mode de connexion mobile doit être défini sur **Auto** pour utiliser la fonction Connection Recovery. Voir aussi **Page Mobile Network, page 46**.

ÉTAPE 3 Entrez les valeurs de **Failover Check Interval**, **Failover Ping Timeout** et **Failover Retry**.

ÉTAPE 4 Choisissez un site sur lequel effectuer la validation de basculement. Sélectionnez **Gateway** (la passerelle par défaut de l'interface) ou entrez l'adresse IP d'un site personnalisé.

ÉTAPE 5 Pour activer l'équilibrage de charge WAN, sélectionnez **Enabled**. l'équilibrage de charge ne peut pas être utilisé si le basculement d'interface est activé.

ÉTAPE 6 Indiquez les valeurs de priorité et de pondération de l'interface WAN telles comme indiqué dans le tableau **Paramètres de configuration multi-WAN.**

ÉTAPE 7 Cliquez sur **Submit** pour enregistrer les paramètres.

Paramètres de configuration multi-WAN

Failover	
Connection Failover	Garantit que la connexion Internet est toujours connectée via un lien WAN stable. **Enabled** : Lorsque cette option est activée, la SRP commence par déterminer l'interface WAN avec la priorité la plus élevée. Si le site de validation associé avec le WAN est inaccessible, la SRP tente d'établir la route par défaut de l'interface du WAN prioritaire suivant s'il est disponible et remplace la route par défaut du système par celle de ce WAN. Lorsque le site de validation associé à l'interface WAN avec la priorité la plus élevée est accessible, la SRP restaure la route par défaut du système comme étant celle de l'interface WAN avec la priorité la plus élevée et arrête la connexion WAN avec la priorité la plus faible. **Disabled** : Une fois désactivées, toutes les interfaces WAN tentent d'établir la connexion, et la route par défaut du système est définie comme étant celle de l'interface WAN avec la priorité la plus élevée. L'équilibrage de charge WAN est configurable dans cet intervalle.
Failover Values	▪ **Failover Check Interval** : Fréquence à laquelle la SRP vérifie l'état de la connexion Internet. La valeur par défaut est 60 secondes. ▪ **Failover Ping Timeout** : Délai maximal autorisé pour la réponse de vérification. La valeur par défaut est 5 secondes. ▪ **Failover Ping Retries** : Nombre de contrôles de vérification non réussis avant le basculement vers l'interface disponible suivante. La valeur par défaut est de 1 seconde. ▪ **Failback after Check Interval Successes** : Nombre de vérifications réussies requises sur une interface restaurée avant que le trafic ne soit redirigé vers celle-ci.

Paramètres de configuration multi-WAN

Connection Validation Site	Adresse IP utilisée comme cible du ping pour la SRP qui détecte l'état de la connexion Internet. Sélectionnez **Gateway** (la passerelle par défaut de l'interface) ou entrez l'adresse IP d'un site **Personnalisé**.
WAN Interface	Affiche les informations relatives à l'état actuel des connexions de réseau mobile filaire. Cliquez sur le lien **Status** pour afficher les détails d'interface ou pour configurer la priorité d'interface à l'aide de la liste déroulante Priority de chaque interface.
WAN Interface Detail	Affiche des informations détaillées sur les interfaces WAN, notamment le nom de l'interface, l'adresse IP, le masque réseau et l'adresse IP de la passerelle.
Load Balance	
WAN Load Balancing	Sélectionnez **Enable** pour activer WAN Load Balancing. La valeur par défaut est Disabled. Une fois cette option activée, nous vous recommandons de désactiver NAT. Pour cela, consultez la section **Traduction d'adresses de réseau (NAT), page 85.** Failover et Load Balancing ne peuvent pas être activés simultanément. L'activation de Failover remplace Load balancing.
Health Check	Sélectionnez **Enable** pour déterminer l'état des interfaces WAN. La valeur par défaut est Disabled. La SRP peut surveiller la validité d'un lien en envoyant des paquets ICMP à la passerelle par défaut de l'interface ou à la passerelle distante personnalisée.
Health Check Time Interval	Entrez la période pendant laquelle la SRP vérifie l'état des interfaces WAN. La valeur par défaut est 60 secondes.
Load Balance Control	Poids multi-WAN utilisés par l'interface WAN pour équilibrer le trafic sortant. La plage est comprise entre 0 et 99. Une valeur 1 par défaut est affectée à toutes les interfaces WAN. Si la valeur est zéro, l'équilibrage de charge n'est pas utilisé.

Configuration des interfaces VLAN et des ports LAN

Cette section décrit la configuration des ports VLAN et LAN de la SRP. Elle comprend les sections suivantes :

- **Page DHCP Server**
- **Page VLAN Settings**
- **Page Port Settings**
- **Page Protocole Spanning Tree Protocol**

Pour accéder à ces pages, cliquez sur **Interface Setup > LAN** à partir de l'utilitaire de configuration.

Page DHCP Server

La page DHCP Server permet de créer des pools de baux DHCP, de réserver des baux pour des hôtes spécifiques, de définir le routage par défaut et les valeurs de l'option DHCP.

Pour configurer la SRP en tant que serveur DHCP, vous devez commencer par créer un serveur DHCP dans la page DHCP Server puis l'activer en l'affectant à une interface VLAN.

REMARQUE Lors de la création d'un serveur DHCP, spécifiez l'adresse IP et le masque de sous-réseau de l'interface VLAN à laquelle le serveur est affecté. Sinon, les options d'adressage IP sont configurées directement via les paramètres VLAN.

ÉTAPE 1 Cliquez sur **Interface Setup > LAN > DHCP Server**. La fenêtre DHCP Server s'ouvre.

ÉTAPE 2 Cette page permet d'afficher, de modifier ou d'ajouter une nouvelle entrée DHCP.

- Pour afficher les détails d'une entrée DHCP, cliquez sur cette entrée dans la liste DHCP. Les informations s'affichent dans le tableau DHCP Details au dessous.
- Pour modifier ou supprimer une entrée DHCP dans la liste DHCP, cliquez sur l'icône en forme de stylet **Edit** ou sur **Delete** (x).
- Pour créer un nouveau pool de serveur DHCP, cliquez sur **Add Entry**. La fenêtre DHCP Server de la nouvelle entrée s'ouvre.

ÉTAPE 3 Configurez les paramètres du serveur DHCP comme indiqué dans le tableau **Paramètres du serveur DHCP** ci-dessous.

ÉTAPE 4 Cliquez sur **Submit** pour enregistrer les paramètres.

Paramètres du serveur DHCP

Router IP	
DHCP Name	Identifie cette configuration de serveur DHCP et sert à affecter le service à une interface VLAN.
Local IP Address/ Subnet Mask	Adresse IP et masque de sous-réseau (8-32 bits) utilisés pour configurer l'interface VLAN à laquelle cette règle DHCP s'applique.
DHCP Server Setting	
DHCP Mode	Choisissez le mode DHCP dans la liste déroulante. Sélectionnez le mode **DHCP Server** ou **DHCP Relay**. L'agent relais DHCP relaie les messages DHCP entre les serveurs DHCP sur les différents réseaux IP. Si vous sélectionnez cette option, saisissez dans le champ **Remote DHCP Server** l'adresse IP à laquelle les messages DHCP seront envoyés. **REMARQUE** Si vous avez choisi le mode DHCP Relay, désactivez manuellement NAT pour le VLAN en cours de configuration. Si vous sélectionnez DHCP Relay, NAT n'est pas désactivé automatiquement. Pour désactiver complètement NAT, consultez la section **Page Global Settings, page 86**. Pour désactiver NAT pour des VLAN spécifiques, consultez la section **Page NAT Bypass, page 87**.
Remote DHCP Server	(Mode DHCP Relay uniquement) Définit l'adresse IP du serveur DHCP qui sert de relais pour les messages DHCP.
IP Reservation	Affiche ou masque les informations de réservation DHCP. Cliquez sur ce bouton pour afficher ou modifier les réservations. Cliquez à nouveau dessus pour masquer les réservations.
Select Clients from DHCP Tables	(Cette option n'est visible que si les réservations IP sont affichées) Affiche les clients qui reçoivent actuellement des adresses IP du serveur DHCP. Pour réserver l'adresse IP actuellement affectée à l'utilisation exclusive d'un client, cochez la case **Select** et cliquez sur le bouton **Add Clients**. Le client s'affiche dans le tableau Clients Already Reserved.

Paramètres du serveur DHCP

Manually Adding Client	(Cette option n'est visible que si les réservations IP sont affichées) Pour réserver une adresse IP pour un client, entrez le nom du client et l'adresse IP à réserver. Saisissez ensuite l'adresse MAC du client et cliquez sur **Add**. Le client s'affiche dans le tableau Clients Already Reserved.
WAN Interface	Choisissez l'interface WAN à partir de laquelle les informations DHCP associées (notamment DNS) sont obtenues.
Default Gateway	Entrez l'adresse IP de la passerelle par défaut à utiliser par les clients de ce pool. Si le champ a la valeur 0.0.0.0, l'adresse IP locale du VLAN sert de passerelle par défaut.
Option 66	Fournit les informations d'adresse du serveur de configuration aux hôtes qui en font la demande. Les informations du serveur sont définies de l'une des trois manières ci-dessous. ▪ **Local TFTP Server** : La SRP utilise son propre serveur TFTP pour alimenter les fichiers de configuration afin qu'ils renvoient sa propre adresse IP locale au client. ▪ **Remote TFTP Server** : Si la SRP a été configurée à l'aide de cette méthode, elle utilise les informations relatives au serveur qu'elle a reçues via Option 66 sur son interface WAN en réponse aux demandes du client local. ▪ **Manual TFTP Server** : Permet la configuration manuelle d'une adresse de serveur de configuration. Bien que cette option soit généralement utilisée pour fournir une adresse IP ou un nom d'hôte complet, la SRP peut aussi accepter et proposer une URL complète (comprenant le protocole, le chemin d'accès et le nom de fichier) pour répondre aux besoins de clients spécifiques.
Option 67	Nom du fichier de configuration/d'amorçage. Utilisée avec Option 66 pour autoriser le client à formuler une demande TFTP appropriée pour le fichier.

Paramètres du serveur DHCP

Option 159	URL de configuration qui définit le protocole et les informations de chemin d'accès à l'aide d'une adresse IP pour les clients qui ne peuvent pas utiliser DNS. Par exemple : **https://10.1.1.1:888/configs/bootstrap.cfg**
Option 160	URL de configuration qui définit le protocole et les informations de chemin d'accès à l'aide d'un nom de domaine complet (FQDN) pour les clients qui peuvent utiliser DNS. Par exemple : **https://myconfigs.cisco.com:888/configs/bootstrap.cfg**
DNS Proxy	Une fois activés, les clients locaux reçoivent l'adresse IP locale SRP à utiliser pour les requêtes DNS. La SRP authentifie ensuite ces requêtes sur les serveurs DNS avec lesquels elle a été configurée. Reportez -vous à la remarque relative à DNS dans la section **Page Internet Option, page 45.** Une fois désactivés, les clients DHCP reçoivent des informations de serveur DNS basées sur les éléments ci-dessous. ▪ Si le champ Static DNS est configuré, seul ce serveur est proposé aux clients. ▪ Si le champ Static DNS n'est pas configuré, jusqu'à trois serveurs sont proposés, d'abord à partir de la configuration statique globale Internet Options et ensuite à partir de l'interface WAN mentionnée ci-dessus.
Starting IP Address	Adresse IP de la première adresse de ce pool.
Maximum DHCP Users	Nombre maximal de périphériques auxquels vous souhaitez que le serveur DHCP affecte des adresses IP. Ce nombre est affecté par le masque de sous-réseau et l'adresse IP de départ et ne peut pas être supérieur à 1 024. La valeur par défaut est 50.
Client Lease Time	Durée pendant laquelle une adresse est louée à un client. Entrez cette durée en minutes. La valeur par défaut est égale à 0 minute, soit une journée. Entrez **9999** pour affecter une durée infinie.

Paramètres du serveur DHCP

Static DNS	Adresse du serveur DNS que les clients DHCP utilisent directement pour la résolution des noms. Cette option n'est nécessaire que si le proxy DNS est désactivé pour ce serveur DHCP. Ce champ est masqué lorsque le proxy DNS est activé.
WINS (Window Internet Naming Service)	Gère la résolution du nom d'hôte pour la résolution d'adresse. Lorsque vous utilisez un serveur WINS, entrez l'adresse IP du serveur. Autrement, ne renseignez pas ce champ.

REMARQUE Le serveur DHCP SRP propose également des informations de domaine aux clients lorsqu'elles sont disponibles. Lorsque la SRP dispose de plusieurs noms de domaine, la valeur configurée de manière statique (Internet Options) est utilisée de préférence à celle indiquée par l'interface de routage par défaut du système. Les noms de domaine indiqués sur d'autres interfaces WAN ne sont pas utilisés pour le protocole DHCP.

Page VLAN Settings

Cette page permet de configurer les paramètres des interfaces Virtual LAN (VLAN).

ÉTAPE 1 Cliquez sur **Interface Setup > LAN > VLAN Settings**. La fenêtre VLAN Settings s'ouvre. Cette page permet d'afficher la liste des VLAN configurés, d'ajouter ou de supprimer un VLAN et d'afficher les informations détaillées relatives à un VLAN sélectionné.

- Pour modifier ou supprimer une entrée VLAN dans VLAN List, cliquez sur l'icône en forme de stylet **Edit** ou sur **Delete** (**x**).
- Pour afficher les informations relatives à une entrée VLAN (pool de serveur DHCP), cliquez sur l'entrée dans VLAN List. Les informations détaillées relatives à l'entrée s'affichent dans le tableau VLAN Details au dessous.
- Pour créer un VLAN, cliquez sur **Add Entry**. La fenêtre VLAN Settings du nouveau VLAN s'ouvre.

ÉTAPE 2 Spécifiez les paramètres VLAN de la nouvelle entrée comme indiqué dans le tableau **Paramètres VLAN**.

ÉTAPE 3 Cliquez sur **Submit** pour enregistrer les paramètres.

Paramètres VLAN

VLAN List	▪ **Name** : La valeur par défaut est data_Lan et voice_Lan. ▪ **ID** : La valeur par défaut est data_Lan : 1 et voice_Lan : 100. ▪ Address Type : La valeur par défaut est data_Lan et voice_Lan : DHCP Server Pool. ▪ **Voice** : La valeur par défaut est data_Lan : désactivé et voice_Lan : activé. ▪ **Membership** : La valeur par défaut est data_Lan : Port LAN 1-4 et SSID1 3, 4, voice_Lan : LAN Port 1-4 et SSID2.
VLAN Name	Entrez un nom pour le VLAN.
VLAN ID	Entrez un numéro d'identification pour le VLAN.
Voice VLAN	Cochez cette case pour que les applications vocales utilisent ce VLAN. La valeur par défaut est data_Lan : désactivé et voice_Lan : activé. L'ensemble du trafic provenant d'un VLAN voix suit la route par défaut vocale spécifiée dans la configuration d'interface WAN à moins qu'un PBR (Policy-Based Routing) soit configuré pour le VLAN voix. Le PBR est prioritaire sur la route par défaut. Il n'existe aucun paramètre QoS implicite pour le VLAN voix. Vous devez créer des paramètres appropriés.
Role	Lors du pontage des ports LAN avec une interface WAN, le rôle de VLAN contrôle la manière dont l'interface IP associée est créée. ▪ **LAN role** : Crée l'interface IP, si nécessaire, sous la forme d'un VLAN LAN. Les VLAN créés sans interfaces WAN sont automatiquement créés avec le rôle LAN. ▪ **WAN role** : Crée l'interface IP sous la forme d'une sous-interface du WAN Ethernet sélectionné. Le VLAN obtenu sera un domaine de diffusion de couche 2 à l'extérieur du pare-feu.

Paramètres VLAN

Address Type	Détermine la manière dont l'interface IP VLAN est configurée. ▪ Sélectionnez **None** si une interface IP n'est pas requise. C'est généralement le cas lorsque seuls les ports sont pontés. ▪ Choisissez **Static IP Address** pour définir manuellement une adresse pour l'interface. ▪ Choisissez **Dynamic IP Address** pour demander une adresse à un serveur DHCP sur le réseau local. ▪ Choisissez **DHCP server** pour activer un service de serveur DHCP configuré précédemment sur cette interface. Dans ce cas, l'adresse IP de VLAN est dérivée de la configuration du serveur DHCP.
Available Interface	Interfaces disponibles pour être ajoutées au VLAN. Pour placer une interface dans la liste Added Interface, cliquez sur cette interface puis sur le **bouton en forme de flèche droite (>)**. Pour déplacer toutes les interfaces en même temps, cliquez sur le **bouton en forme de double flèche droite (>>)**.
Added Interface	Interfaces qui étaient sélectionnées comme membres du pont VLAN. Pour supprimer une interface de la liste, cliquez sur cette interface puis sur le **bouton en forme de flèche gauche (<)**. Pour supprimer toutes les interfaces en même temps, cliquez sur le **bouton en forme de double flèche gauche (<<)**.

Page Port Settings

La page Port Settings permet de définir les attributs de port du VLAN et de modifier ou d'afficher les paramètres de port.

ÉTAPE 1 Cliquez sur **Interface Setup > LAN > Port Settings**. La fenêtre Port Settings s'ouvre.

ÉTAPE 2 Indiquez les paramètres de contrôle de flux et de vitesse/mode duplex pour les ports LAN 1-4 comme indiqué dans le tableau **Paramètres de ports**.

ÉTAPE 3 Pour afficher les informations relatives à un port, cliquez sur un élément de la liste des ports. Des informations détaillées sur le port s'affichent dans le tableau Port Details au dessous.

ÉTAPE 4 Pour modifier une entrée de port, cliquez sur l'icône en forme de stylet **Edit**. La fenêtre VLAN Port Settings s'ouvre.

ÉTAPE 5 Indiquez les paramètres de ports comme indiqué dans le tableau **Paramètres de ports**.

ÉTAPE 6 Cliquez sur **Submit** pour enregistrer les paramètres.

Paramètres de ports

Mode	Comportement actuellement configuré du port. ▪ **Desktop mode** : Fournit aux périphériques connectés l'accès à un VLAN données unique pour lequel la SRP fournit des services. L'ensemble du trafic sera non balisé. ▪ **IP Phone + Desktop mode** : Le port est configuré avec un VLAN données pour l'accès natif et un VLAN voix pour être utilisé avec un téléphone IP connecté. Le protocole CDP est utilisé pour communiquer les informations du VLAN voix au téléphone. Cela implique qu'il n'existe que deux VLAN associés à ce port, un pour les données qui est le VLAN natif et l'autre qui est le VLAN voix et qui est uniquement balisé. ▪ **Switch/AP mode** : Le port est configuré pour s'intégrer à plusieurs VLAN (toute combinaison autre que 1 VLAN données et 1 VLAN voix) afin de créer des liaisons avec un commutateur ou un point d'accès sans fil. ▪ **Generic** : Le port est configuré uniquement pour le pontage au niveau de la couche 2.
Enabled Flow Control	Mécanisme permettant d'arrêter temporairement la transmission de données sur cette interface physique. Par exemple : il peut arriver qu'une station émettrice (ordinateur) transmette des données plus rapidement que d'autres parties du réseau (notamment la station réceptrice) peuvent accepter. L'élément de réseau submergé envoie une trame PAUSE, qui suspend la transmission de l'expéditeur pendant une durée spécifiée. Pour activer cette fonctionnalité, cochez la case **Enabled Flow Control**. La valeur par défaut est Disabled.

Paramètres de ports

Speed Duplex	Choisissez le mode duplex dans la liste déroulante. Sélectionnez **Auto-negotiate**, **10 Half**, **10 Full**, **100 Half** **100 Full**, **1000 Half** ou **1000 Full**. La valeur par défaut est Auto-negotiate.
Port Details	Affiche les informations détaillées de chaque port configuré.

Paramètres de port de VLAN

Port	Indiquez les paramètres de sécurisation du port pour la qualité de service. La valeur par défaut est untrusted. ▪ **Untrusted** : Si le port n'est pas sécurisé, la classe de service du trafic Ethernet sera marquée avec le paramètre de priorité configuré. ▪ **Trust** : Si le port est sécurisé, les marquages de la classe de service en entrée sont conservés pour la mise en file d'attente (qui peut ou non se produire ultérieurement lorsque le paquet traverse le routeur).
Port/Access VLAN	Sélectionnez le VLAN natif (PVID) de ce port. La liste déroulante comprend tous les identifiants de VLAN qui ont été configurés dans la page VLAN Settings.
Priority	Permet de définir une priorité pour le trafic non marqué ou non sécurisé reçu sur ce port. Par défaut, la priorité est définie sur 0. Un chiffre supérieur indique une priorité supérieure.
Voice VLAN	Lorsque le mode VLAN est IP Phone + Desktop, l'identifiant du VLAN voix est affiché. Cette valeur n'est indiquée qu'à titre d'information.

Page Protocole Spanning Tree Protocol

La page STP permet de configurer les paramètres du protocole STP (Spanning Tree Protocol). STP est un protocole réseau de couche liaison qui permet une topologie sans boucle pour les LAN avec ponts. La fonction de base de STP est d'éviter les boucles de pont et de garantir le rayonnement de la diffusion.

ÉTAPE 1 Cliquez sur Interface **Setup > LAN > STP**. La fenêtre STP s'ouvre.

ÉTAPE 2 Pour activer STP, sélectionnez **Enabled**. La valeur par défaut est Disabled.

ÉTAPE 3 Indiquez les paramètres STP des ports LAN 1-4 comme il est indiqué ci-dessous.

- **Enabled STP** : sélectionnez les ports qui participeront à STP. Vérifiez que ce paramètre est activé pour les connexions avec les liaisons de commutateur.
- **Path Cost** : Si cette option est définie sur Auto-detect, la SRP utilise un coût du chemin du port basé sur la configuration de son débit. Pour remplacer cette valeur, décochez l'option Auto-detect et entrez une valeur comprise entre 0 et 240.

ÉTAPE 4 Si nécessaire, configurez les paramètres avancés STP comme indiqué dans le tableau **Paramètres STP**.

ÉTAPE 5 Cliquez sur **Submit** pour enregistrer les modifications.

REMARQUE Forward Delay, Hello Time et Max Age sont les paramètres de configuration transmis par le pont racine à tous les autres ponts pour définir la configuration STP actuelle. Si la SRP n'est pas élu en tant que racine, les valeurs de minuteur actives peuvent être différentes de celles configurées ici. Les calculs de temps sont basés sur la norme IEEE 802.1D qui fournit l'interopérabilité avec les ponts traditionnels. Cela provient du fait que les minuteurs sont déterminés depuis le pont racine. Un pont impose les relations suivantes :

(2 x Forward_Delay - 1,0 seconde) >= Max_Age
Max_Age >= 2 (x + Hello_Time 1,0 seconde

Paramètres STP

Advanced Settings	
Bridge Priority	Cette option est utilisée pour influencer le choix du pont qui devient la racine STP. Le pont avec la valeur la plus faible du réseau est élu racine. Les priorités de pont admises sont comprises entre 0 et 61 440, par paliers de 4 096. La valeur par défaut est 32 768.

Paramètres STP

Forward Delay	Temps passé à l'écoute et l'état d'apprentissage. Ce temps est égal à 15 secondes par défaut, mais vous pouvez le régler entre 4 et 30 secondes.
Hello Time	Intervalle entre chaque envoi par un pont d'une BPDU (Bridge Protocol Data Unit). Ce temps est égal à 2 secondes par défaut, mais vous pouvez le régler entre 1 et 10 secondes.
Max Age	Minuteur qui définit la durée d'attente des ponts lorsqu'ils ont reçu le dernier message hello pour supposer que la topologie de couche 2 a été modifiée. À ce stade, la configuration actuelle de Spanning Tree est ignorée et la nouvelle topologie est détectée. Ce temps est égal à 20 secondes par défaut, mais vous pouvez le régler entre 6 et 40 secondes.

Configuration d'un LAN sans fil

Cette section décrit le paramétrage d'un LAN sans fil pour la SRP. Elle comprend les sections suivantes :

- **Page Basic Wireless Settings**
- **Page Wi-Fi Protected Setup**
- **Page Wireless MAC Filter**
- **Page Advanced Wireless Settings**
- **Page Wi-Fi Multimedia Setting**

Pour accéder à ces pages, cliquez sur **Interface Setup > Wi-Fi Settings** à partir de l'utilitaire de configuration.

Page Basic Wireless Settings

La page Basic Wireless Settings permet de configurer le point d'accès sans fil intégré à la SRP et jusqu'à quatre réseaux sans fil.

ÉTAPE 1 Cliquez sur **Interface Setup > Wi-Fi Settings > Basic Wireless Settings**. La fenêtre Basic Wireless Settings s'ouvre.

ÉTAPE 2 Configurez les paramètres de réseau sans fil comme indiqué dans le tableau **Paramètres sans fil de base. Lorsque vous avez terminé, cliquez sur Submit** pour enregistrer vos paramètres.

ÉTAPE 3 Sélectionnez le mode réseau pour activer le sans fil et cliquez sur **Apply**.

REMARQUE Le sans fil doit être activé pour utiliser la fonction WPS (Wi-Fi Protected Setup).

ÉTAPE 4 Configurez les paramètres de sécurité réseau pour chaque SSID. Dans la zone Wireless Table, cliquez sur le bouton **Edit** dans la colonne Security. La fenêtre Wireless Security s'ouvre.

ÉTAPE 5 Choisissez la valeur du mode de sécurité dans la liste déroulante. La valeur par défaut est Disabled.

Lorsque vous activez le mode de sécurité, une fenêtre s'ouvre qui permet de définir les paramètres de sécurité de ce mode (type d'authentification, cryptage, mot de passe, etc.). Entrez les paramètres de sécurité comme indiqué dans le tableau **Paramètres sans fil de base**, puis cliquez sur **Submit** pour enregistrer vos paramètres.

> **REMARQUE** L'algorithme par défaut correspondant aux paramètres du mode de sécurité WPA et WAP2 (Personal et Enterprise) est AES. Étant donné que le cryptage AES est une méthode de cryptage renforcée, nous vous recommandons d'utiliser dans la mesure du possible AES au lieu de TKIP.

Paramètres sans fil de base

Network Mode	Choisissez le mode sans fil en fonction du type de périphérique de votre réseau. **REMARQUE** Le point d'accès sans fil est désactivé par défaut pour garantir la sécurité du réseau. Vous devez sélectionner un mode de réseau actif pour l'activer avant de poursuivre la configuration. ▪ **Mixed :** Choisissez cette option si vous avez des périphériques Sans fil N, Sans fil G et Sans fil B sur votre réseau. ▪ **BG-Mixed** : Choisissez cette option si vous avez uniquement des périphériques Sans fil G et Sans fil B sur votre réseau. ▪ **Wireless-N Only :** Choisissez cette option si vous avez uniquement des périphériques Sans fil N. ▪ **Wireless-G Only** : Choisissez cette option si vous avez uniquement des périphériques Sans fil G. ▪ **Wireless-B Only** : Choisissez cette option si vous avez uniquement des périphériques Sans fil B. ▪ **Disabled :** Choisissez cette option si vous ne voulez pas utiliser le point d'accès sans fil intégré.
Radio Band	Sélectionnez la bande passante sans fil de votre réseau. Trois options sont disponibles : Auto, Standard–20MHz Channel et Wide-40MHz Preferred. L'option par défaut est Standard–20MHz Channel. La configuration de canal large bande est disponible uniquement pour les réseaux et clients Sans fil-N. Si le mode de canal large bande est sélectionné pour les réseaux mixtes, l'utilisation du canal standard reste disponible pour les clients Sans fil B et Sans fil G.
Wide Channel	Si vous avez sélectionné le canal Wide-40MHz Channel pour le paramètre Radio Band, ce paramètre est alors disponible pour votre canal sans fil N principal. Sélectionnez un canal (3-9 pour les modèles A, 3-11 pour les modèles E) dans la liste déroulante. Si la bande radio est sélectionnée automatiquement, le canal large bande est également sélectionné automatiquement.

Paramètres sans fil de base

Standard Channel	Si vous avez sélectionné Wide-40MHz Preferred ou Standard -20MHz Channel pour le paramètre Radio Band, ce paramètre est disponible. Sélectionnez le canal pour la mise en réseau Sans fil N, Sans fil G et Sans fil B. Si vous avez sélectionné Wide-40MHz Preferred pour le paramètre Radio Band, le canal Standard est un canal auxiliaire pour le Sans fil N. La valeur par défaut est Standard Channel 11 - 2.462 GHZ (Wide Channel 9). Si la bande radio est sélectionnée automatiquement, le canal standard sera également choisi automatiquement.
Wireless Table	
Wireless Network Name (SSID)	Nom du réseau que les clients utilisent pour se connecter au réseau. Par défaut, le réseau sans fil s'appelle « cisco-data » et est connecté au VLAN par défaut. Pour renommer le réseau sans fil par défaut, entrez un nom de réseau sans fil unique, sensible à la casse et ne dépassant pas 32 caractères. Vous pouvez utiliser tous les caractères du clavier). Le second réseau sans fil par défaut s'appelle par défaut « cisco-voice » et est ponté au VLAN voix. Pour créer un second réseau sans fil, saisissez un nom de réseau sans fil unique dans le paramètre SSID2. Pour activer ce réseau, sélectionnez **Enabled Network**. **REMARQUE** Votre ISP ou votre fournisseur de services téléphoniques Internet peut être chargé de contrôler les paramètres SSID2. Pour plus d'informations, contactez votre ISP ou votre fournisseur de services téléphoniques Internet.
SSID 1/2/3/4	Nom de réseau partagé parmi tous les périphériques d'un réseau sans fil. La SRP peut prendre en charge jusqu'à quatre réseaux sans fil. Par défaut, le premier et le deuxième réseau sans fil sont activés. Pour chaque réseau sans fil, configurez le nom du réseau sans fil (SSID), le nom du réseau de diffusion et l'option Enable Network. **REMARQUE** Guest Network utilise SSID3. N'utilisez pas SSID3 si vous prévoyez d'utiliser cette fonctionnalité.

Paramètres sans fil de base

Broadcast Network Name	Lorsque les clients sans fil recherchent les réseaux sans fil disponibles sur le réseau local, ils détectent les SSID diffusés par les réseaux sans fil proches. Pour diffuser le SSID, laissez la case cochée. Pour ne pas diffuser le SSID, décochez cette case. Les utilisateurs sans fil devront alors connaître le SSID à associer au réseau.
Enabled Network	Pour activer le réseau sans fil, cochez cette case. Pour désactiver le réseau sans fil, décochez cette case.
WPS Hardware Button	Appuyez sur le bouton Wi-Fi Protected Setup sur le panneau avant de la SRP pour associer le SSID actuellement sélectionné. Pour utiliser cette fonctionnalité, le SSID doit être activé. Sinon, il est grisé. Pour activer WPS, consultez la section **Page Wi-Fi Protected Setup, page 71.** **REMARQUE** La fonctionnalité Wi-Fi Protected Setup ne prend pas en charge les modes de sécurité WPA et WPA2 Enterprise.

Paramètres de sécurité sans fil

Pour accéder à ces paramètres, cliquez sur le bouton **Edit Security** pour les SSID configurés)	
Security Mode	Choisissez une valeur **Security Mode** pour votre réseau sans fil. La SRP prend en charge les modes de sécurité WPA Personal, WPA Enterprise, WPA2 Personal, WPA2 Enterprise et WEP. (WPA, acronyme de Wi-Fi Protected Access, désigne une norme de sécurité plus puissante que le système de cryptage WEP.) WEP est l'acronyme de Wired Equivalent Privacy (confidentialité équivalente aux réseaux câblés). Pour ne pas utiliser la sécurité sans fil, conservez la valeur par défaut Disabled. Nous vous recommandons d'utiliser le niveau de sécurité le plus élevé pris en charge par vos périphériques clients sans fil.
WEP Security Mode Settings	
WEP	Méthode de cryptage de base, qui n'est pas aussi sécurisée que WPA. Cette méthode peut être requise si vos périphériques réseau ne prennent pas en charge WPA.

Paramètres de sécurité sans fil

Authentication Type	Choisissez **Auto** ou **Shared Key** dans la liste déroulante. Lorsque le paramètre Auto est activé, le réseau est ouvert et n'importe quel périphérique peut s'y connecter avec ou sans clé partagée. L'authentification par clé partagée nécessite que le client fournisse la clé que vous spécifiez dans cette page.
Encryption	Sélectionnez un niveau de cryptage WEP, **64-bit 10 hex digits or 5 ASCII characters** (par défaut) ou **128-bit 26 hex digits or 13 ASCII characters**. Des niveaux supérieurs de cryptage offrent des niveaux accrus de sécurité, mais en raison de la complexité du cryptage, ils peuvent réduire les performances réseau.
Passphrase	Saisissez un mot de passe pour générer automatiquement les clés WEP. Cliquez ensuite sur le bouton **Generate**. Les clés valides s'affichent.
Key 1-4	Si vous n'avez pas saisi de mot de passe, saisissez la ou les clés WEP manuellement. Si vous choisissez le cryptage WEP 64 bits, la clé doit contenir exactement 5 ou 10 caractères hexadécimaux. Si vous choisissez le cryptage WEP 128 bits, la clé doit contenir exactement 13 ou 26 caractères hexadécimaux. Les caractères hexadécimaux valides sont « 0 » à « 9 » et « A » à « F ». **REMARQUE** La SRP prend en charge une clé WEP unique pour le point d'accès. Si plusieurs SSID sont configurés avec le cryptage WEP, ils doivent partager la même clé.
TX Key	Sélectionnez la clé TX (Transmit) à utiliser. La valeur par défaut est 1.
WPA Personal Mode Settings	
WPA Personal	Fournit une sécurité sans fil accrue avec un cryptage avancé (TKIP ou AES).
WPA Algorithms	Prend en charge deux méthodes de cryptage, TKIP et AES, avec des clés de cryptage dynamiques. Sélectionnez le type d'algorithme, **AES** ou **TKIP**. La valeur par défaut est AES.
WPA Shared Key	Saisissez un mot de passe composé de 8 à 63 caractères.

Paramètres de sécurité sans fil

Group Key Renewal	Saisissez un intervalle en secondes pour indiquer la fréquence à laquelle la SRP change les clés de cryptage. La valeur par défaut de ce champ est de 3 600 secondes (1 heure).
WPA2 Personal Mode Settings	
WPA2 Personal	Fournit une sécurité sans fil accrue avec un cryptage avancé (AES ou TKIP + AES).
WPA Algorithms	Prend en charge deux méthodes de cryptage, TKIP et AES, avec des clés de cryptage dynamiques. Sélectionnez le type d'algorithme, **AES** ou **TKIP + AES**. La valeur par défaut est AES.
WPA Shared Key	Saisissez un mot de passe composé de 8 à 63 caractères.
Group Key Renewal	Saisissez un intervalle en secondes pour indiquer la fréquence à laquelle la SRP change les clés de cryptage. La valeur par défaut de ce champ est de 3 600 secondes (1 heure).
WPA and WPA2 Enterprise Settings **REMARQUE** La fonctionnalité Wi-Fi Protected Setup ne prend pas en charge les modes de sécurité WPA et WPA2 Enterprise.	
WPA Enterprise	Cette option comporte le mode WPA utilisé avec un serveur RADIUS accessible. Si vous avez deux serveurs RADIUS, sélectionnez-en un comme serveur principal et indiquez un serveur secondaire à utiliser en tant que serveur de sauvegarde.
WPA2 Enterprise	Cette option comporte le mode WPA2 utilisé avec un serveur RADIUS accessible. Si vous avez deux serveurs RADIUS, sélectionnez-en un comme serveur principal et utilisez le serveur secondaire comme serveur de sauvegarde.
WPA Algorithms	WPA et WPA2 prennent en charge deux méthodes de cryptage, TKIP et AES, avec des clés de cryptage dynamiques. Sélectionnez l'algorithme à utiliser : **TKIP** ou **AES**. La valeur par défaut est AES.
Primary RADIUS Server	**RADIUS Server** : Saisissez l'adresse IP du serveur RADIUS. **RADIUS Port** : Entrez le numéro de port du serveur RADIUS. La valeur par défaut est 1812. **Shared Secret** : Entrez la clé partagée entre la SRP et le serveur. Cette clé peut comporter entre 8 et 63 caractères ASCII ou 64 caractères hexadécimaux.

Paramètres de sécurité sans fil

Secondary RADIUS Server	**RADIUS Server Address** : Saisissez l'adresse IP du serveur RADIUS. **RADIUS Port** : Entrez le numéro de port du serveur RADIUS. **Shared Secret** : Entrez la clé partagée entre la SRP et le serveur. Cette clé peut comporter entre 8 et 63 caractères ASCII ou 64 caractères hexadécimaux.
Key Renewal Timeout	Saisissez un intervalle en secondes pour indiquer la fréquence à laquelle la SRP change les clés de cryptage. La valeur par défaut de ce champ est de 3 600 secondes (1 heure). La plage est comprise entre 600 et 7200 secondes.

Page Wi-Fi Protected Setup

La page Wi-Fi Protected Setup (WPS) permet de configurer automatiquement la sécurité sans fil pour les réseaux sans fil.

REMARQUE Vérifiez que le périphérique client WPS est situé à proximité de la SRP lors de la configuration.

ÉTAPE 1 Cliquez sur **Interface Setup > Wi-Fi Settings > Wi-Fi Protected Setup**. La fenêtre Wi-Fi Protected Setup s'ouvre.

ÉTAPE 2 Pour activer la fonctionnalité Wi-Fi Protected Setup pour un SSID, choisissez le nom du réseau sans fil à configurer dans la liste déroulante. Le SSID données par défaut est cisco-data. Le SSID voix par défaut est cisco-voice.

La fonctionnalité Wi-Fi Protected Setup est activée par défaut. Sélectionnez **Disabled** pour ne pas utiliser cette fonctionnalité pour le VLAN sélectionné.

ÉTAPE 3 Sélectionnez une méthode de la fonctionnalité Wi-Fi Protected Setup. Pour obtenir une description des méthodes, consultez la section **Méthodes Wi-Fi, page 72**. Utilisez la méthode qui s'applique au périphérique client que vous avez configuré.

ÉTAPE 4 Une fois la configuration terminée, l'état actuel Wi-Fi Protected s'affiche en bas de la page.

Méthodes Wi-Fi

Il existe trois méthodes pour configurer la fonctionnalité Wi-Fi Protected Setup :

Méthode Wi-Fi Protected Setup 1

Utilisez cette méthode si votre périphérique client dispose d'un bouton WPS.

ÉTAPE 1 Cliquez ou appuyez sur le bouton **WPS** sur le périphérique client.

ÉTAPE 2 Cliquez sur l'icône **WPS** de cette page ou appuyez sur le bouton WPS sur la façade avant de la SRP si cet élément a été associé à un SSID actuellement sélectionné. Voir aussi **Page Basic Wireless Settings, page 65.**

ÉTAPE 3 Une fois le périphérique client configuré, cliquez sur **OK**. Pour plus d'instructions, consultez votre périphérique client ou sa documentation.

Méthode Wi-Fi Protected Setup 2

Utilisez cette méthode si votre périphérique client a un code PIN WPS.

ÉTAPE 1 Entrez le code PIN dans le champ figurant dans cette page puis cliquez sur **Register**.

ÉTAPE 2 Une fois le périphérique client configuré, cliquez sur **OK**. Pour plus d'instructions, consultez votre périphérique client ou sa documentation.

Méthode Wi-Fi Protected Setup 3

Utilisez cette méthode si le périphérique client demande le code PIN de la SRP.

ÉTAPE 1 Entrez le code PIN répertorié dans cette page. (Il est également indiqué sur l'étiquette située au bas de la SRP.)

ÉTAPE 2 Une fois le périphérique client configuré, cliquez sur **OK**. Pour plus d'instructions, consultez votre périphérique client ou sa documentation.

Page Wireless MAC Filter

La page Wireless MAC filter permet de spécifier les adresses MAC des périphériques sans fil dont l'accès est autorisé ou bloqué par la SRP.

ÉTAPE 1 Cliquez sur **Interface Setup > Wi-Fi Settings > Wireless MAC Filter**. La fenêtre Wireless MAC Filter s'ouvre.

ÉTAPE 2 Dans la liste déroulante Select a SSID, choisissez les paramètres de filtre MAC à appliquer au SSID. Le SSID données par défaut est cisco-data. Le SSID voix par défaut est cisco-voice.

ÉTAPE 3 Pour filtrer les utilisateurs sans fil par adresse MAC pour autoriser ou bloquer leur accès, sélectionnez **Enable**. La valeur par défaut est Disable.

ÉTAPE 4 Dans la zone Access Restriction, sélectionnez **Prevent** ou **Permit**.

ÉTAPE 5 Si Wireless MAC Filter est activé, cliquez sur le bouton **Show Client List** pour ouvrir la page Wireless Client List. Cette page affiche les ordinateurs et autres périphériques actuellement associés au réseau sans fil. Vous pouvez trier la liste par nom de client, adresse IP, adresse MAC et état.

ÉTAPE 6 Sélectionnez **Save to MAC Address Filter List** pour n'importe quel périphérique à ajouter à la liste et cliquez sur **Add**. Cliquez sur le bouton **Refresh** (Actualiser) pour obtenir des informations actualisées. Pour quitter cette page et revenir à la page Wireless MAC Filter, cliquez sur **Close**.

REMARQUE Vous pouvez filtrer l'accès sans fil à l'aide des adresses MAC des périphériques sans fil qui émettent dans le rayon d'action de votre réseau.

ÉTAPE 7 Cliquez sur **Submit** pour enregistrer les paramètres.

Paramètres de Wireless MAC Filter

Wireless MAC Filter	
Select a SSID	Nom du réseau sans fil à configurer. Le SSID données par défaut est cisco-data. Le SSID voix par défaut est cisco-voice.
Wireless MAC Filter	Pour filtrer les utilisateurs sans fil par adresse MAC pour autoriser ou bloquer leur accès, sélectionnez **Enable**. La valeur par défaut est Disable.

Paramètres de Wireless MAC Filter

Access Restriction	
Prevent	Bloque l'accès sans fil des clients répertoriés dans la table d'adresses MAC. Il s'agit du paramètre par défaut.
Permit	Autorise l'accès sans fil uniquement pour les clients répertoriés dans la table d'adresses MAC.
Show Client List	Affiche la liste des ordinateurs et autres périphériques connectés à ce réseau sans fil. Pour ajouter un client répertorié dans la zone MAC Address Table, cochez la case **Save to MAC Address Filter List** et cliquez sur **Add**. Pour masquer la liste des clients, cliquez sur **Hide Client List**.
MAC Address Table	
01-32	Entrez les adresses MAC des périphériques dont vous souhaitez bloquer ou autoriser l'accès sans fil.

Page Advanced Wireless Settings

La page Wireless Settings permet de configurer les fonctions sans fil avancées de la SRP.

REMARQUE Ces paramètres doivent être configurés par un administrateur expérimenté. Avant de configurer ces paramètres, vérifiez que le mode sans fil est activé sur la SRP. Voir aussi **Page Basic Wireless Settings, page 65**.

ÉTAPE 1 Cliquez sur **Interface Setup > Wi-Fi Settings > Advanced Wireless Settings**. La fenêtre Advanced Wireless s'ouvre.

ÉTAPE 2 Pour configurer le seuil RTS, sélectionnez un SSID dans la liste déroulante.

ÉTAPE 3 Saisissez une valeur dans le champ RTS Threshold. Si vous êtes confronté à un flux de données incohérent, n'effectuez que de légères réductions. La valeur par défaut recommandée est 2 347.

ÉTAPE 4 Modifiez les paramètres de la zone Global Settings comme indiqué dans le tableau **Paramètres sans fil avancés.**

ÉTAPE 5 Cliquez sur **Submit** pour enregistrer les paramètres.

Paramètres sans fil avancés

Advanced Wireless Setup	
Select a SSID	Nom du réseau sans fil à configurer. Le SSID données par défaut est cisco-data. Le SSID voix par défaut est cisco-voice.
RTS Threshold	La SRP transmet des trames RTS (Request to Send) à une station réceptrice et négocie l'envoi d'une trame de données. Après la réception d'un signal RTS, la station sans fil répond par une trame CTS pour autoriser le lancement de la transmission. Si vous êtes confronté à un flux de données incohérent, vous pouvez adapter ce seuil. Seule une légère réduction de la valeur par défaut (2347) est recommandée. Si la taille d'un paquet du réseau est inférieure à la taille prédéfinie du seuil RTS, le mécanisme RTS/CTS n'est pas activé. Le seuil RTS doit conserver sa valeur par défaut de 2347.
Global Settings	
AP Isolation	Isole tous les clients et périphériques sans fil les uns des autres. Les périphériques sans fil peuvent communiquer avec la SRP mais pas avec d'autres périphériques sans fil sur le réseau. Pour utiliser cette fonction, sélectionnez **Enabled**. L'option AP Isolation est désactivée par défaut.
Basic Rate	Série de débits avec lesquels la SRP peut transmettre des données. La SRP signale son débit de base aux autres périphériques sans fil de votre réseau afin qu'ils connaissent les débits utilisés, et sélectionnent automatiquement le meilleur débit de transmission. Le paramètre par défaut est Default, ce qui permet à la SRP de prendre en charge tous les débits de transmission sans fil standard (1-2 Mbits/s, 5,5 Mbits/s, 11 Mbits/s, 18 Mbits/s et 24 Mbits/s). Les autres options sont 1-2 Mbits/s pour les anciennes technologies sans fil et All, qui permet à la SRP de prendre en charge tous les débits du sans fil. Le paramètre Basic Rate n'indique pas le débit réel de transmission des données. Pour spécifier le débit de transmission de données de la SRP, configurez le paramètre Transmission Rate.

Paramètres sans fil avancés

Transmission Rate	Permet de définir le débit de transmission des données en fonction du débit de votre réseau sans fil. Choisissez l'un des débits de transmission proposés ou sélectionnez l'option **Auto** pour demander à la SRP d'adopter automatiquement le débit de transmission le plus rapide possible et d'activer la fonctionnalité Auto-Fallback. Cette fonctionnalité détermine le meilleur débit de connexion possible entre la SRP et un client sans fil. La méthode par défaut est Auto.
CTS Protection Mode	La SRP utilise automatiquement le mode de protection CTS (Clear-To-Send, prêt à émettre) lorsque les produits sans fil N et G rencontrent des problèmes graves et ne parviennent pas à transmettre des données à la SRP dans un environnement à fort trafic 802.11b. Cette fonction renforce la capacité de la SRP à intercepter l'ensemble des transmissions sans fil N et G, mais peut impacter les performances. La valeur par défaut est Auto.
DTIM Interval	Indique l'intervalle du DTIM (Delivery Traffic Indication Message). Un champ DTIM est un champ de compte à rebours qui informe les clients de la prochaine fenêtre à utiliser pour écouter les messages de diffusion ou de multidiffusion. Lorsque la SRP met ces messages en mémoire tampon pour les clients associés, elle envoie le prochain DTIM avec une valeur d'intervalle DTIM. Ses clients sont informés par les balises et se préparent à recevoir les messages de diffusion et de multidiffusion. La plage est comprise entre 255 et la valeur par défaut est 1.
Fragmentation Threshold	Spécifie la taille maximale d'un paquet avant la fragmentation des données en plusieurs paquets. Si le taux d'erreurs de paquet est élevé, vous pouvez augmenter légèrement le seuil de fragmentation. Un seuil de fragmentation trop bas peut affecter les performances du réseau. Seule une légère diminution de la valeur par défaut est recommandée. Dans la plupart des cas, il est préférable de conserver la valeur par défaut 2346.

Paramètres sans fil avancés

Beacon Interval	Indique l'intervalle de fréquence de la balise. Une balise est un paquet diffusé par la SRP pour synchroniser le réseau sans fil. Saisissez une valeur comprise entre 40 et 3 500 millisecondes. La valeur par défaut est 100.
Power Control	Choisissez **high**, **middle** ou **low** pour spécifier la plage du réseau sans fil. La valeur par défaut est high, ce qui correspond à un niveau de puissance normal.

Page Wi-Fi Multimedia Setting

La page WMM Setting permet de configurer la prise en charge des périphériques Wi-Fi Multimedia (WMM) sur votre réseau.

ÉTAPE 1 Cliquez sur **Interface Setup > Wi-Fi Settings > WMM Setting**. La fenêtre WMM Setting s'ouvre.

ÉTAPE 2 Si d'autres périphériques de votre réseau prennent en charge WMM, conservez le paramètre par défaut **Enabled**.

ÉTAPE 3 Pour l'option No Acknowledgement, sélectionnez **Enabled** pour désactiver la fonctionnalité d'accusé de réception afin que la SRP ne renvoie pas de données si une erreur se produit. La valeur par défaut est Disabled.

ÉTAPE 4 Cliquez sur **Submit** pour enregistrer les paramètres.

Utilisation de l'interface de gestion

La page Management Interface permet de définir les interfaces de bouclage, qui peuvent être utilisées pour les mises à jour de routage et certains protocoles. Vous pouvez configurer deux interfaces de bouclage.

ÉTAPE 1 Cliquez sur **Interface Setup > Management Interface**. La fenêtre Management Interface s'ouvre.

Cette page permet d'afficher ou de modifier les interfaces de bouclage actuellement configurées.

ÉTAPE 2 Pour modifier une interface, cliquez sur l'icône en forme de stylet **Edit**. La fenêtre Manually Adding Loopback s'ouvre.

ÉTAPE 3 Entrez l'adresse IP à utiliser pour l'interface de bouclage. L'adresse ne doit pas chevaucher une autre interface configurée sur la SRP.

REMARQUE L'adresse IP utilisée pour l'interface de bouclage suppose que le masque de sous-réseau est 255.255.255.255.

ÉTAPE 4 Cliquez sur **Submit** pour enregistrer les paramètres.

5

Configuration du réseau

Ce chapitre décrit la configuration des paramètres réseau pour les plates-formes prêtes pour les services. Il comprend les sections suivantes :

- **Routage**
- **Traduction d'adresses de réseau (NAT)**
- **Qualité de service**
- **Firewall**
- **Relais PPPoE**
- **DNS dynamique**
- **Configuration DMZ**
- **Protocole de gestion des groupes Internet (IGMP)**
- **Universal Plug and Play**
- **Cisco Discovery Protocol**
- **Réseau invité**
- **Usurpation d'adresse DNS**

Pour accéder à ces pages, cliquez sur **Network Setup** dans la barre de menu de l'utilitaire de configuration.

Routage

Cette section décrit comment configurer les différents types de routage sur la plate-forme prête pour les services, notamment :

- **Page Static Routes**
- **Page Routing Information Protocol**
- **Page Intervlan Routing**
- **Page Policy Routing**

Pour accéder à ces pages, cliquez sur **Network Setup > Routing** dans l'utilitaire de configuration.

Page Static Routes

Utilisez la page Static Routes pour configurer des itinéraires statiques pour le trafic réseau.

ÉTAPE 1 Cliquez sur **Network Setup > Routing > Static Routes**. La fenêtre Static Routes s'ouvre. Cette page vous permet d'ajouter un itinéraire, de modifier un itinéraire ou de consulter les itinéraires existants dans la table de routage.

ÉTAPE 2 Pour ajouter un itinéraire statique, cliquez sur **Add Entry**.

ÉTAPE 3 Complétez les champs **Route Name**, **Destination** et **Subnet Mask** pour le réseau ou l'hôte spécifié, auquel vous souhaitez attribuer un itinéraire statique.

ÉTAPE 4 Dans le champ **Gateway**, saisissez l'adresse IP de la passerelle qui permet le contact entre la plate-forme SRP et le réseau ou l'hôte spécifié, ou sélectionnez l'interface pour cet itinéraire dans la liste déroulante.

ÉTAPE 5 Cliquez sur **Submit** pour enregistrer les modifications.

REMARQUE Pour afficher la table de routage pour tous les itinéraires spécifiés, cliquez sur le bouton **Show Routing Table**. Pour masquer ces informations, cliquez sur le bouton une nouvelle fois.

Paramètres du routage statique

Enter Route Name	Nom de l'itinéraire statique.
Destination	Adresse IP du réseau ou de l'hôte auquel vous souhaitez attribuer un itinéraire statique.
Subnet Mask	Détermine quelle partie d'une adresse IP correspond à la partie réseau et quelle partie correspond à la partie hôte.
Gateway	Adresse IP du périphérique passerelle qui permet le contact entre la plate-forme SRP et le réseau ou l'hôte.
Interface	Indique si l'adresse IP de destination se trouve sur le LAN et sur un réseau sans fil (réseaux filaires et sans fil internes) ou sur Internet (WAN).
Show Routing Table	Affiche la table de routage pour tous les itinéraires spécifiés.

Page Routing Information Protocol

Utilisez les pages du protocole RIP (Routing Information Protocol) pour configurer le routage dynamique sur la plate-forme SRP. Vous pouvez activer ce protocole pour permettre aux interfaces spécifiées de s'ajuster automatiquement aux modifications physiques apportées à la structure du réseau et d'échanger les tables de routage avec d'autres routeurs. La plate-forme SRP détermine l'itinéraire des paquets réseau en sélectionnant le plus petit nombre de sauts entre la source et la destination.

ÉTAPE 1 Cliquez sur **Network Setup > Routing > RIP**. La fenêtre RIP s'ouvre.

ÉTAPE 2 Pour activer le protocole RIP (routage dynamique), sélectionnez **Enabled**. La valeur par défaut est Disabled.

ÉTAPE 3 Si le protocole RIP est activé, sélectionnez la version du protocole RIP et les délais d'expiration.

ÉTAPE 4 Sélectionnez les réseaux qui participeront au protocole de routage, par interface ou par réseau, à l'aide du champ **Interface** ou **Network** (adresse IP et masque de sous-réseau).

- Si vous avez choisi la « RIP By Interface », spécifiez les paramètres d'interface, tels que définis dans le tableau **Paramètres RIP** ci-dessous.
- Si vous avez choisi « RIP By Network », cliquez sur le bouton **Add Network** et spécifiez l'adresse du réseau dans le champ **Network Address**, ainsi que le masque pour la nouvelle entrée.

ÉTAPE 5 Cliquez sur Submit pour enregistrer les paramètres.

Paramètres RIP

Version RIP	Pour limiter les types de paquets qui peuvent être transmis, sélectionnez **Version 1** ou **Version 2**. Vous pouvez également sélectionner **RIP v1/v2** pour permettre la transmission des paquets de version 1 et 2.
RIP Timer	Minuteurs qui régulent les performances RIP. Ils incluent un minuteur de mise à jour de routage, un minuteur de délai d'expiration d'itinéraire et un minuteur d'annulation de routage. **Update** : spécifiez le taux d'envoi de mises à jour de routage par la plate-forme SRP. La valeur par défaut est 30 secondes. **Timeout** : spécifiez le taux auquel la plate-forme SRP compte recevoir des mises à jour de routage à partir de chaque routeur dans la table de routage. La valeur par défaut est 180 secondes. Si cette valeur est dépassée, l'itinéraire est déclaré inaccessible. L'itinéraire est supprimé de la table de routage seulement à l'expiration du minuteur d'annulation de routage. **Flush** : spécifiez la durée maximale pendant laquelle la plate-forme SRP peut attendre une mise à jour avant de supprimer un itinéraire de la table de routage. La valeur par défaut est 120 secondes.
RIP By	Sélectionnez **RIP by Interface** ou **RIP by Network**.

Paramètres RIP

RIP List	Affiche les paramètres du protocole RIP de toutes les interfaces SRP. Si vous avez sélectionné l'option « RIP by Interface », vous pouvez modifier une interface en cliquant sur l'icône en forme de stylet **Edit** à côté de l'interface que vous souhaitez modifier. **Interface :** indique le type d'interface. **RIP Enabled** : indique si le protocole RIP est activé ou désactivé sur l'interface. Cochez la case pour activer le protocole RIP. **Passive Mode** : Tous les paquets de réception sont traités comme à l'ordinaire et envoient uniquement des paquets RIP de multidiffusion ou de monodiffusion aux voisins RIP. Pour sélectionner ce mode, sélectionnez **Enabled** dans la fenêtre RIP Config Edit. **Authentication** : si vous envoyez et recevez des paquets RIP de version 2, sélectionnez une authentification RIP sur une interface. La plate-forme SRP prend en charge deux modes d'authentification sur une interface : l'authentification par mot de passe simple et l'authentification MD5. Un mot de passe simple ou MD5 peut être toute chaîne de 15 caractères au maximum. Vous pouvez utiliser des lettres et des chiffres ASCII en plus des caractères., -_ **REMARQUE** La version 1 du protocole RIP ne prend pas en charge l'authentification.
RIP Network	Si vous avez sélectionné l'option « RIP By Network », cliquez sur le bouton **Add Network** et spécifiez l'adresse IP et le masque de sous-réseau pour l'entrée.

Page Intervlan Routing

La configuration de réseaux VLAN aide à contrôler la taille du domaine de diffusion et maintient local le trafic local. Toutefois, lorsqu'une station terminale d'un réseau VLAN doit communiquer avec une station terminale d'un autre réseau VLAN, une communication entre réseaux locaux virtuels est requise. Cette communication est rendue possible par le routage entre réseaux locaux virtuels.

REMARQUE Le routage entre réseaux locaux virtuels ne s'applique pas au réseau VLAN invité si vous avez configuré l'accès invité sans fil.

ÉTAPE 1 Cliquez sur **Network Setup > Routing > Intervlan Routing**. La fenêtre Intervlan Routing s'ouvre.

ÉTAPE 2 Le routage entre réseaux locaux virtuels est activé par défaut. Pour la désactiver, sélectionnez **Disable**.

ÉTAPE 3 Cliquez sur **Submit** pour enregistrer les modifications, si nécessaire.

Page Policy Routing

Utilisez la page Policy Routing pour acheminer le trafic en fonction des critères correspondants. Le trafic qui arrive aux interfaces LAN sélectionnées est classé en fonction d'un set de règles prioritaires et est acheminé vers une interface WAN choisie en conséquence.

ÉTAPE 1 Cliquez sur **Network Setup > Routing > Policy Routing**. La fenêtre Policy Routing s'ouvre. Cette page vous permet de consulter, ajouter, modifier et hiérarchiser les règles de routage.

ÉTAPE 2 Pour ajouter une règle de routage, cliquez sur **Add Entry**. La fenêtre Policy Routing Rule add correspondant à la nouvelle règle s'ouvre.

ÉTAPE 3 Définissez les critères de correspondance, tels que définis dans le tableau **Paramètres de stratégie de routage** ci-dessous. Configurez uniquement les champs qui suffisent à classer correctement le trafic.

ÉTAPE 4 Pour désactiver cette règle en cas d'interruption de l'interface, cochez la case **Disable Rule**. La désactivation d'une règle permet à l'algorithme de correspondance de sélectionner un itinéraire alternatif en cas d'échec de liaison. Si vous laissez la règle activée et qu'un échec de la liaison se produit, le trafic correspondant est ignoré.

ÉTAPE 5 Si nécessaire, ajustez la priorité de chaque règle pour satisfaire vos conditions requises de correspondance spécifiques.

ÉTAPE 6 Cliquez sur **Submit** pour enregistrer les modifications.

Paramètres de stratégie de routage

Incoming Interface	Spécifiez quelles interfaces LAN recevront le trafic entrant dans la liste déroulante Incoming Interface. Sélectionnez Any ou l'une des interfaces VLAN actuellement définies.
Source IP Address and Destination IP Address/Subnet Mask	Spécifiez les adresses IP source et de destination, ainsi que les masques de sous-réseau correspondants, pour lesquelles la règle doit s'appliquer.
Port	Sélectionnez le port de destination auquel cette règle doit s'appliquer. « Any » est le paramètre par défaut. Si vous choisissez **Single** ou **Range**, spécifiez le numéro de port ou la plage de numéros de ports dans les champs appropriés.
Protocol	Limitez le protocole IP (**TCP** ou **UDP**) pour la mise en correspondance du trafic, si nécessaire.
DSCP	Spécifiez la valeur DSCP à respecter pour cette règle.
Route	Spécifiez l'itinéraire WAN vers lequel le trafic correspondant sera envoyé. Choisissez un tunnel IPSec, un tunnel GRE ou une interface WAN quelconque configuré(e).

Traduction d'adresses de réseau (NAT)

Cette section décrit comment configurer les paramètres de traduction d'adresses de réseau (NAT) pour la plate-forme SRP. Il comprend les sections suivantes :

- **Page Global Settings**
- **Page NAT Bypass**
- **Page Port Forwarding**
- **Page Port Range Triggering**

Pour accéder à ces pages, cliquez sur **Network Setup > NAT** dans l'utilitaire de configuration.

Page Global Settings

Utilisez la page NAT pour activer ou désactiver le routage NAT, qui permet à la plate-forme SRP d'héberger votre connexion réseau à Internet.

ÉTAPE 1 Cliquez sur **Network Setup > NAT> NAT Setting**. La fenêtre NAT Setting s'ouvre.

ÉTAPE 2 Le routage NAT est activé par défaut et appliqué à l'ensemble du trafic passant entre les interfaces LAN et WAN. Pour désactiver complètement le routage NAT, cliquez sur **Disabled**.

ÉTAPE 3 Spécifiez les paramètres de contrôle de passerelle de couche d'applications (ALG), tels qu'ils sont définis dans le tableau **Paramètres ALG** ci-dessous. Pour activer une passerelle ALG, cliquez sur **Enabled** à côté de la passerelle ALG que vous souhaitez utiliser.

REMARQUE Toutes les passerelles ALG sont activées par défaut.

ÉTAPE 4 Cliquez sur Submit pour enregistrer les paramètres.

Paramètres ALG

NAT	Le routage NAT est activé par défaut (il s'agit du paramètre recommandé pour un périphérique d'accès à Internet). Sélectionnez **Disabled** si la plate-forme SRP sera utilisée dans un réseau privé avec d'autres routeurs.
SIP ALG	Lorsque cette option est activée, la passerelle ALG permet au trafic SIP de transiter par le processus NAT en traduisant les informations d'adresse et de port intégrées à partir du réseau interne privé en une adresse IP publique du périphérique.
NetMeeting	Offre une prise en charge pour Microsoft Netmeeting et d'autres applications H.323 via NAT en traduisant les informations d'adresse et de port intégrées.
RTSP ALG	Garantit que les flux UDP RTSP et RTP transitent par le processus NAT.

Paramètres ALG

IRC ALG	Extension couramment utilisée pour appeler le protocole DCC (Direct Client-to-Client). Cela permet aux utilisateurs de s'envoyer des fichiers entre-eux, ainsi que de discuter entre-eux sans avoir recours à un serveur. L'envoi DCC est utilisé partout où vous envoyez des fichiers via IRC. DCC Chat est le plus souvent utilisé par les robots Eggdrop. Si vous utilisez le routage NAT, cette extension vous permet d'envoyer des fichiers et de lancer des discussions. **REMARQUE :** Vous n'avez pas besoin de cette extension pour récupérer des fichiers, lancer des discussions ou effectuer d'autres tâches dans IRC.

Page NAT Bypass

Dans de nombreux cas, l'utilisation du routage NAT pour l'ensemble du trafic LAN vers WAN est suffisante. Dans certains cas, quand plusieurs services sont fournis via des connexions de réseau étendu logiques ou physiques différentes, il peut être nécessaire de traduire l'adressage pour certaines connexions et d'effectuer un routage sans traduction pour d'autres.

La fonction de contournement du routage NAT permet de définir des exceptions à la fonctionnalité NAT globale (voir **Page Global Settings, page 86**), garantissant que le trafic qui respecte les critères spécifiés est acheminé sans traduction d'adresses.

ÉTAPE 1 Cliquez sur **Network Setup > NAT > NAT Bypass**. La fenêtre NAT Bypass s'ouvre.

Cette page permet de consulter une stratégie existante, de modifier une stratégie ou d'ajouter une nouvelle stratégie.

ÉTAPE 2 Pour ajouter une nouvelle stratégie, cliquez sur **Add Policy**. La fenêtre NAT Bypass s'ouvre.

ÉTAPE 3 Spécifiez un nom pour la nouvelle stratégie.

ÉTAPE 4 Sélectionnez **Enabled** pour activer la stratégie. La valeur par défaut est Disabled.

ÉTAPE 5 Spécifiez les critères de règle en définissant d'où provient le trafic à acheminer (interface interne) et où il va (interface externe).

REMARQUE Le trafic local est mis en correspondance lorsqu'il provient d'un réseau VLAN localement défini, de l'adresse IP d'un hôte spécifique ou d'un réseau indirect local (un réseau IP accessible via un autre routeur connecté au LAN d'une plate-forme SRP).

ÉTAPE 6 Cliquez sur **Submit** pour enregistrer les paramètres.

ÉTAPE 7 La nouvelle stratégie apparaît dans la table Policy List à la page NAT Bypass. Cliquez sur une stratégie pour afficher les détails de la stratégie.

Paramètres de contournement du routage NAT

Détails de la stratégie	
Policy Name	Spécifiez un nom pour la nouvelle stratégie.
Enabled	Cliquez sur **Enabled** pour activer la stratégie.
Interface interne	
Interface VLAN	Choisissez l'**interface VLAN** d'où proviendra le trafic à acheminer.
Host IP Address	Définissez le trafic par l'adresse IP de l'hôte source.
Indirect Network	Spécifiez l'**adresse IP** source et le **masque de sous-réseau** associés au réseau indirect.
Interface externe	
Interface WAN	Choisissez une **interface WAN** disponible pour l'interface externe dans le menu déroulant.
IP Address/Subnet Mask	Spécifiez l'**adresse IP** de destination et le **masque de sous-réseau** vers lesquels le trafic doit être acheminé et non traduit.

Page Port Forwarding

Utilisez la page Port Forwarding si votre réseau local héberge des services réseau (applications Internet), tels que le Web, la messagerie électronique, le FTP, la vidéoconférence ou les jeux. Pour chaque service, le trafic Internet est transféré par application (port IP) aux serveurs locaux qui hébergent ces services.

Le transfert de port permet à la plate-forme SRP d'acheminer les paquets adressés à une adresse IP de réseau WAN pour un port ou une plage de ports d'application spécifique, vers un périphérique sur le réseau local. Par exemple, si vous disposez d'un serveur Web sur le LAN d'une plate-forme SRP, vous pouvez configurer le transfert de port pour toutes les demandes adressées au port 80 qui seront traduites et envoyées à l'adresse IP du serveur Web interne.

REMARQUE Pour garantir un transfert correct du trafic, les serveurs locaux doivent être configurés avec une adresse IP statique ou une adresse IP réservée via DHCP doit leur être attribuée. Utilisez la page **Interface Setup > LAN > DHCP Server** pour réserver des adresses IP. Voir aussi **Page DHCP Server, page 54.**

ÉTAPE 1 Cliquez sur **Network Setup > NAT > Port Forwarding**. La fenêtre Port Forwarding s'ouvre. Cette page vous permet de consulter une entrée, de modifier une entrée ou d'ajouter une entrée pour un autre service réseau.

ÉTAPE 2 Pour ajouter une nouvelle entrée, cliquez sur **Add Entry**. La fenêtre Manually Adding Port Forwarding s'ouvre.

ÉTAPE 3 Saisissez les paramètres de transfert de port, tels qu'ils sont définis dans le tableau **Paramètres de transfert de port**.

ÉTAPE 4 Cliquez sur **Submit** pour enregistrer les paramètres.

Paramètres de transfert de port

Port Forwarding Type	Sélectionnez le type de transfert de port dans la liste déroulante. **Single Port Forwarding** : transfère le trafic pour un port spécifié vers le même port ou vers un port alternatif sur le serveur cible dans le LAN. **Port Range Forwarding :** transfère le trafic pour une plage de ports vers les mêmes ports sur le serveur cible dans le LAN. Pour connaître les ports ou plages de ports requis, reportez-vous à la documentation de l'application Internet.
Application Name	(Pour le transfert de port unique seulement) Choisissez une application courante dans la liste déroulante, telle que Telnet ou DNS. Pour spécifier une application qui n'est pas dans la liste, sélectionnez **Add a new name**, puis entrez le nom de la nouvelle application.

Paramètres de transfert de port

Enter a Name	(Pour le transfert de port unique seulement) Spécifiez le nom de la nouvelle application.
WAN Interface Name	Sélectionnez l'interface WAN à laquelle le trafic est adressé initialement.
External Port	(Pour le transfert de port unique seulement) Spécifiez le numéro de port que les clients externes utiliseront pour configurer une connexion avec le serveur interne.
Internal Port	(Pour le transfert de port unique seulement) Spécifiez le numéro de port que la plate-forme SRP utilise lors du transfert du trafic vers le serveur interne. Pour des raisons de simplicité, les numéros de ports externes et internes sont souvent identiques ; cependant, des numéros de ports externes différents peuvent être utilisés pour différencier le trafic du même type d'application, destiné à différents serveurs internes, ou pour promouvoir la confidentialité grâce à l'utilisation de ports non standard.
Start-End Port	(Transfert de plage de ports uniquement) Spécifiez la plage des ports utilisés par le serveur ou l'application Internet. Spécifiez le premier port dans la première case et le port final dans la seconde case pour spécifier la plage. Pour plus d'informations, reportez-vous à la documentation de l'application Internet. Dans ce cas, les numéros de ports ne sont pas modifiés lorsqu'ils sont transférés vers le serveur interne.
Protocol	Protocoles à transférer : **TCP**, **UDP** ou **les deux**.
IP Address	Adresse IP du serveur local qui recevra le trafic transféré.
Enabled	Cliquez sur **Enabled** pour activer cette règle de transfert. Par défaut, l'option est désélectionnée (désactivée).

Page Port Range Triggering

Utilisez la page Port Range Triggering pour permettre à la plate-forme SRP de surveiller les données sortantes pour des numéros de ports spécifiques et de créer, de manière dynamique, une règle de transfert pour diriger le trafic de retour vers le client local demandeur.

Le déclenchement d'une plage de ports n'exige pas que le client local utilise une adresse IP fixe. Le trafic pour tout port donné peut uniquement être transféré à un client local à la fois.

ÉTAPE 1 Cliquez sur **Network Setup > NAT > Port Range Triggering**. La fenêtre Port Range Triggering s'ouvre. Cette page vous permet de consulter les entrées existantes depuis la liste du déclenchement d'une plage de ports, ainsi que les détails d'une entrée sélectionnée.

ÉTAPE 2 Pour ajouter une nouvelle entrée pour le déclenchement d'une plage de ports, cliquez sur **Add Entry**. La fenêtre Port Range Triggering pour la nouvelle entrée s'ouvre.

ÉTAPE 3 Entrez les paramètres pour le déclenchement d'une plage de ports, tels qu'ils sont définis dans le tableau **État de déclenchement d'une plage de ports ci-dessous.**

ÉTAPE 4 Cliquez sur **Submit** pour enregistrer les paramètres.

État de déclenchement d'une plage de ports

Application Name	Entrez un nom pour identifier l'application dans la liste du déclenchement d'une plage de ports.
WAN	Choisissez l'interface **WAN** via laquelle les ports de déclenchement seront détectés.
LAN	Choisissez le **LAN** dans lequel l'ordinateur hôte se trouve et vers lequel le trafic transféré sera dirigé.
Triggered Range	Spécifiez les numéros de ports **de début** et **de fin** de la plage de ports déclenchés. Lorsqu'un client local établit une connexion sortante avec un port de cette plage, la plate-forme SRP ouvre les ports qui sont spécifiés dans les champs Forwarded Range par le client de départ. Reportez-vous à la documentation de l'application Internet pour connaître les numéros de ports appropriés.

État de déclenchement d'une plage de ports

Forwarded Range	Entrez les numéros de ports **de début** et **de fin** de la plage de ports transférés. Ces ports sont ouverts lorsqu'une connexion sortante est établie à l'un des ports spécifiés dans les champs Triggered Range. Reportez-vous à la documentation de l'application Internet pour connaître les numéros de ports appropriés.
Protocol	Sélectionnez un type de protocole dans la liste déroulante (**TCP**, **UDP** ou **les deux**).
Enabled	Cliquez sur **Enabled** pour activer les applications que vous avez définies. Cette option est désactivée par défaut.

Qualité de service

Cette section décrit comment configurer les paramètres de qualité de service (QoS) pour la plate-forme SRP. Il comprend les sections suivantes :

- **Page QoS Bandwidth Control**
- **Page QoS Policy**
- **Page CoS To Queue**
- **Page DSCP To Queue**

Pour accéder à ces pages, cliquez sur **Network Setup > QoS** dans la barre de menu de l'utilitaire de configuration.

Page QoS Bandwidth Control

Utilisez la page QoS Bandwidth Control pour permettre à la plate-forme SRP d'évaluer les transmissions de données ascendantes limites afin de s'adapter au service haut débit.

ÉTAPE 1 Cliquez sur **Network Setup > QoS > Bandwidth Control**. La fenêtre QoS Bandwidth Control s'ouvre.

ÉTAPE 2 Cliquez sur **Enabled** en regard de l'interface sur laquelle vous souhaitez activer le contrôle de la bande passante. Décochez la case pour désactiver l'option. La valeur par défaut est Disabled.

ÉTAPE 3 Pour configurer la bande passante disponible pour chaque interface physique, cliquez sur l'icône en forme de stylet **Edit**. La fenêtre Bandwidth Shaping Control s'ouvre.

ÉTAPE 4 Spécifiez les valeurs de contrôle de mise en forme de la bande passante, telles qu'elles sont définies dans le tableau **Paramètres de contrôle de mise en forme de la bande passante ci-dessous.**

ÉTAPE 5 Cliquez sur **Submit** pour enregistrer les paramètres.

Paramètres de contrôle de mise en forme de la bande passante

Upstream Bandwidth	Spécifiez la valeur maximale de **bande passante en amont** disponible pour le service haut débit connecté. Les valeurs par défaut sont de 100 000 Kbits/s pour les interfaces Ethernet, 1 000 Kbits/s pour les interfaces ADSL_PVC0/1/2/3, 2 000 Kbits/s pour les interfaces 3G et 100 000 Kbits/s pour les interfaces Gigabit Ethernet en mode WAN. **REMARQUE** Définir une valeur plus élevée que la bande passante de service disponible peut entraîner une interruption arbitraire du trafic dans le réseau du fournisseur d'accès.
Strict High Priority Queue	Entrez la bande passante nécessaire pour le trafic à priorité stricte. Le trafic de la file d'attente stricte compris dans ce taux est transmis avant celui de toute autre file d'attente. La plage correspond à 1-70 000 Kbits/s. La valeur par défaut est 128 Kbits/s.

Paramètres de contrôle de mise en forme de la bande passante

High, Medium, Normal, Low	Spécifiez la priorité relative, ou pondération, des files d'attentes de priorité élevée, moyenne, normale et basse. La pondération de la file d'attente détermine la quantité relative de bande passante qui sera garantie pour le trafic de chaque file d'attente pendant les périodes d'activité soutenue. La colonne de la bande passante fournit une indication de la valeur permettant la bande passante à priorité stricte. Pour régler la pondération relative des files d'attente, cliquez sur le bouton plus **(+)** et le bouton moins **(-)**. La plage des priorités est 1-99. En l'absence de trafic à priorité stricte, les données de ces files d'attente sont traitées sur la base du Round Robin pondéré. Les valeurs de bande passante de cette page indiquent le débit minimal garanti disponible par file d'attente, en charge. Des débits de trafic supérieurs sont observés, lorsque les autres files d'attente sont sous-utilisées.

Page QoS Policy

La qualité de service (QoS) assure un meilleur service au trafic réseau prioritaire, ce qui peut concerner des applications en temps réel exigeantes en ressources, telles que les applications de vidéoconférence.

Utilisez la page QoS Policy pour configurer des règles pour classer, mettre en file d'attente et marquer le trafic passant des interfaces LAN aux interfaces WAN. Plusieurs méthodes de classification sont fournies pour garantir la possibilité de hiérarchiser le trafic de manière adéquate.

ÉTAPE 1 Cliquez sur **Network Setup > QoS > QoS Policy**. La fenêtre QoS Policy s'ouvre.

Cette page vous permet de consulter, ajouter et modifier les stratégies QoS. Cliquez sur n'importe quelle règle pour afficher les informations détaillées sur la stratégie.

ÉTAPE 2 Pour ajouter une nouvelle stratégie, cliquez sur **Add Entry**. La fenêtre QoS Priority Setting s'ouvre.

ÉTAPE 3 Sélectionnez la catégorie QoS dans la liste déroulante (**Application**, **MAC Address**, **Ethernet Port**, **VLAN** ou **IP Address**).

ÉTAPE 4 Spécifiez les paramètres de stratégie pour la catégorie spécifique, tels qu'ils sont définis dans le tableau **Paramètres de stratégie QoS : Classification ci-dessous.**

ÉTAPE 5 Sélectionnez les paramètres de mise en file d'attente et de marquage pour cette règle.

REMARQUE Lorsque vous définissez la priorité, n'attribuez pas la valeur High à toutes les applications. Cela annule l'objectif visé avec l'allocation de la bande passante disponible.

ÉTAPE 6 Cliquez sur **Submit** pour enregistrer les paramètres.

Paramètres de stratégie QoS : Classification

Catégorie Application	
Applications/ Name	Choisissez une application standard dans la liste déroulante. Pour spécifier une application non répertoriée, sélectionnez **Add a New Application**, puis entrez le nom de la nouvelle application.
LAN	Choisissez le LAN source. Sélectionnez **All** (Tout) ou l'une des interfaces LAN actuellement définies.
Port Range	Spécifiez le port, ou la plage de ports, et le protocole (**TCP**, **UDP** ou **les deux**) qui définissent l'application requise. Vous pouvez spécifier jusqu'à trois plages de ports par règle. Des ports uniques peuvent être définis en spécifiant la même valeur pour les champs de début et de fin de plage. Pour plus d'informations, reportez-vous à la documentation de l'application Internet.
Catégorie Adresse MAC	
Name	Spécifiez un nom pour décrire cette règle.
LAN	Choisissez le LAN source. Sélectionnez **All** (Tout) ou l'une des interfaces LAN actuellement définies.
MAC Address	Entrez l'**adresse MAC** du périphérique source au format suivant : xx:xx:xx:xx:xx:xx
Catégorie Port Ethernet	
Name	Spécifiez un nom pour décrire cette règle.
LAN	Choisissez le LAN source.

Paramètres de stratégie QoS : Classification

Ethernet	Choisissez le port Ethernet source.
Catégorie VLAN	
Name	Spécifiez un nom pour décrire cette règle.
VLAN	Choisissez le réseau VLAN source.
Catégorie Adresse IP	
Name	Spécifiez un nom pour décrire cette règle.
Destination IP Address	Entrez l'adresse IP de destination qui doit être utilisée pour classer le trafic.
Destination Mask	Entrez le masque de sous-réseau pour la plage IP de l'adresse de destination.

Paramètres de stratégie QoS : Mise en file d'attente

Priority	Choisissez la priorité de mise en file d'attente pour le trafic correspondant : Strict, High, Medium, Normal ou Low.

Paramètres de stratégie QoS : Marquage

Marking	Modifie le champ DiffServ ou CoS du paquet classé par cette règle de stratégie QoS (par plage de ports, MAC, port Ethernet, VLAN et adresse IP de l'application). Pour définir ou remplacer le marquage QoS pour le trafic satisfaisant cette règle, sélectionnez Enabled. Le paramètre par défaut est Disabled, ce qui laisse les marquages QoS inchangés. **CoS** : spécifiez la valeur de classe de service Ethernet entre 0 et 7. Cette valeur est valide uniquement pour les interfaces WAN Ethernet et les PVC ADSL configurés pour le marquage 802.1Q. **DiffServ** : spécifiez les valeurs DSCP (DiffServ Code Point) au format hexadécimal. Les valeurs doivent être comprises entre 0x00 et 0xfc sous forme de multiples de 0x04 et sont valides pour toutes les interfaces WAN IP. Reportez-vous à la table de mappage DiffServe ci-dessous.

Mappages DSCP

Hex	Décimal	Bits DSCP		Mappage de file d'attente suggéré
0x00	0	000000	Par défaut	Normal
0x20	8	001000	CS1	Low
0x28	10	001010	AF11	Low
0x30	12	001100	AF12	Low
0x38	14	001110	AF13	Low
0x40	16	010000	CS2	Low
0x48	18	010010	AF21	Normal
0x50	20	010100	AF22	Normal
Ox58	22	010110	AF23	Normal
0x60	24	011000	CS3	Normal
0x68	26	011010	AF31	Medium
0x70	28	011100	AF32	Medium
0x78	30	011110	AF33	Medium
0x80	32	100000	CS4	Medium
0x88	34	100010	AF41	Medium
0x90	36	100100	AF42	Medium
0x98	38	100110	AF43	Medium
0xa0	40	101000	CS5	Medium
0xB8	46	101110	EF	Strict
0xc0	48	110000	CS6	High
Oxe0		111000	CS7	High

Page CoS To Queue

Utilisez la page CoS To Queue pour mettre en file d'attente le trafic en fonction des paramètres de classe de service (CoS) Ethernet.

ÉTAPE 1 Cliquez sur **Network Setup > QoS > CoS To Queue**. La fenêtre CoS To Queue s'ouvre.

Les valeurs de priorité (0-7) sont mappées sur la file d'attente de la plate-forme SRP, où zéro correspond à la priorité la plus basse et 7 à la priorité la plus élevée. Ces valeurs définissent le type de services, tel que vidéo ou voix.

Les services sont exprimés par le biais du champ PCP à 3 bits dans un en-tête IEEE 802.1Q ajouté à la trame. La façon dont le trafic est traité, lorsqu'il est attribué à une classe particulière quelconque, est non définie et est laissée à la mise en œuvre. L'IEEE a émis quelques recommandations vastes, telles qu'elles sont définies dans le tableau **Valeurs de priorité CoS vers file d'attente** ci-dessous.

ÉTAPE 2 Modifiez la priorité pour chaque classe de service VLAN, selon les besoins. Choisissez un **niveau de priorité** (strict, élevé, moyen, normal ou bas) dans la liste déroulante.

ÉTAPE 3 Cliquez sur **Submit** pour enregistrer les paramètres.

Valeurs de priorité CoS vers file d'attente

Médecin de premier recours	Priorité réseau	Caractéristiques du trafic
1	0 (la plus basse)	Contexte
0	1	Trafic au mieux
2	2	Disponibilité maximum
3	3	Applications critiques
4	4	Vidéo, latence < 100 ms
5	5	Voix, latence < 10 ms
6	6	Contrôle d'interconnexion de réseaux
7	7 (la plus élevée)	Contrôle du réseau

Page DSCP To Queue

Utilisez la page DSCP to Queue pour mettre en file d'attente le trafic en fonction de la valeur du point de code de services différenciés (DSCP) dans le paquet entrant.

ÉTAPE 1 Cliquez sur **Network Setup > QoS > DSCP To Queue**. La fenêtre DSCP To Queue s'ouvre.

ÉTAPE 2 Modifiez les paramètres de priorité pour chaque valeur DiffServ IP, selon les besoins. Choisissez un **niveau de priorité** (strict, élevé, moyen, normal ou bas) dans la liste déroulante. La priorité définit la file d'attente de transfert du trafic sur laquelle le trafic doté de la valeur DSCP doit être mappé.

ÉTAPE 3 Cliquez sur **Submit** pour enregistrer les paramètres.

Firewall

Cette section décrit comment configurer les paramètres de pare-feu pour la plate-forme SRP. Il comprend les sections suivantes :

- **Page Firewall Filter**
- **Page Internet Access Control**
- **Page Advanced Firewall Settings**
- **Relais PPPoE**

Pour accéder à ces pages, cliquez sur **Network Setup > Firewall** dans l'utilitaire de configuration.

Page Firewall Filter

Utilisez la page Firewall Filter pour activer le filtrage de protection pare-feu WAN vers LAN sur la plate-forme SRP. Le pare-feu améliore la sécurité réseau et utilise la fonctionnalité SPI (Stateful Packet Inspection) pour analyser les paquets de données entrant dans votre réseau.

ÉTAPE 1 Cliquez sur **Network Setup > Firewall > Firewall Filter**. La fenêtre Firewall s'ouvre.

ÉTAPE 2 La protection pare-feu SPI est activée par défaut. Pour la désactiver, cliquez sur **Disabled**.

ÉTAPE 3 Spécifiez les options de filtre Web et Internet, telles qu'elles sont définies dans le tableau **Paramètres de filtre de pare-feu ci-dessous.**

ÉTAPE 4 Cliquez sur **Submit** pour enregistrer les paramètres.

Paramètres de filtre de pare-feu

SPI Firewall Protection (Protection par pare-feu SPI)	La protection pare-feu SPI est activée par défaut. Pour la désactiver, cliquez sur **Disabled**.
Options de filtre Internet	
Filter Anonymous Internet Requests	Empêche votre réseau d'être sondé par test Ping ou détecté par d'autres utilisateurs Internet. Cette option permet également de masquer vos ports réseau. Ces deux mesures de protection permettent d'entraver les tentatives d'infiltration de votre réseau par des utilisateurs externes. Ce filtre est activé par défaut. Sélectionnez **Disabled** pour autoriser les requêtes Internet anonymes.
Filter Internet NAT Redirection	Empêche les clients locaux d'accéder aux services locaux via les règles de transfert de port actives (c.-à-d. que les clients locaux ne peuvent pas utiliser l'adresse IP publique du routeur pour accéder aux services locaux, comme ils le pourraient s'ils étaient connectés via Internet). Cette fonctionnalité n'empêche pas un client local d'accéder à un service local directement à l'aide de l'adressage privé. Par défaut, ce filtre est désactivé. Sélectionnez **Enabled** pour filtrer la redirection NAT Internet.
Filter IDENT (Port 113)	Empêche le port 113 d'être analysé par les périphériques situés hors de votre réseau local. Sélectionnez **Enabled** pour filtrer le port 113 ou **Disabled** pour le désactiver.
Filter DoS Attack	Protège la plate-forme SRP contre les attaques de déni de service.

Paramètres de filtre de pare-feu

Paramètres de filtre Web	
Proxy	L'utilisation de serveurs proxy WAN peut compromettre votre sécurité réseau. L'activation du filtre proxy bloque l'accès à tout serveur proxy WAN. Pour activer le filtrage proxy, cochez la case **Proxy**. Par défaut, ce filtre est désactivé.
Java	Java est un langage de programmation pour les sites Web. Le filtrage Java empêche l'accès aux sites Internet créés à l'aide de ce langage de programmation. Pour activer le filtrage Java, cochez la case **Java**. Par défaut, ce filtre est désactivé.
ActiveX	ActiveX est un langage de programmation pour sites Web. Le filtrage ActiveX empêche l'accès aux sites Internet qui utilisent ce langage de programmation. Pour activer le filtrage ActiveX, cochez la case **ActiveX**. Par défaut, ce filtre est désactivé.
Cookies	Les cookies sont des blocs de données stockés sur votre ordinateur et utilisés par les sites Internet lorsque vous interagissez avec eux. Pour filtrer les cookies, cochez la case **Cookies**. Par défaut, ce filtre est désactivé.
Filter Port	Entrez le numéro du port HTTP qui sera analysé lorsque vous utiliserez l'un des filtres ci-dessus. Par défaut, ce paramètre correspond au port 80.

Page Internet Access Control

Utilisez la page Internet Access Control pour configurer les règles de contrôle de l'accès utilisateur à Internet (LAN vers WAN).

ÉTAPE 1 Cliquez sur **Network Setup > Firewall > Internet Access Control**. La fenêtre Internet Access Control s'ouvre. Cette fenêtre vous permet d'ajouter une stratégie, de modifier une stratégie et de consulter une stratégie existante.

ÉTAPE 2 Pour ajouter une stratégie d'accès à Internet, cliquez sur **Add Entry**. La fenêtre Internet Access Control settings pour la nouvelle stratégie s'ouvre.

ÉTAPE 3 Spécifiez un nom pour la stratégie d'accès à Internet.

ÉTAPE 4 Cliquez sur **Enabled** pour activer le contrôle d'accès à Internet. La valeur par défaut est Disabled.

ÉTAPE 5 Vous pouvez appliquer la règle à tout le trafic en sélectionnant **From All**, **To All**, ou vous pouvez limiter la règle afin qu'elle s'applique uniquement à des interfaces spécifiques, telles que From VLAN1 to WAN1.

ÉTAPE 6 Vous pouvez également choisir de cliquer sur **Show Edit List** pour afficher les stratégies d'adresse MAC, d'adresse IP et de plage d'adresses IP.

ÉTAPE 7 Dans la zone Schedule, sélectionnez les jours et les heures pendant lesquels vous souhaitez que cette stratégie soit appliquée. Sélectionnez les différents jours ou sélectionnez **Everyday**. Entrez une plage d'heures en indiquant l'heure de début (**From**) et l'heure de fin (**To**) ou sélectionnez **24 Hours**.

ÉTAPE 8 Sélectionnez les autres options de blocage requises, telles qu'elles sont définies dans le tableau **Paramètres de contrôle d'accès à Internet ci-dessous.**

ÉTAPE 9 Cliquez sur **Submit** pour enregistrer les paramètres.

Paramètres de contrôle d'accès à Internet

Enter Policy Name	Spécifiez un nom pour la stratégie.
Status	Pour activer cette stratégie, cliquez sur **Enabled**. Par défaut, l'option est désactivée.
From, To	Vous pouvez appliquer la règle à tout le trafic en sélectionnant **From All**, **To All**, ou vous pouvez limiter la règle afin qu'elle s'applique uniquement à des interfaces spécifiques, telles que From VLAN1 to WAN1.
Applied PCs (facultatif)	Pour appliquer la stratégie uniquement à des PC spécifiés, cliquez sur le bouton **Show Edit List**. Spécifiez ensuite les différents PC en entrant leur adresse MAC ou leur adresse IP. Vous pouvez spécifier des groupes de PC en entrant jusqu'à deux plages d'adresses IP.
Programmation	
Days	Sélectionnez les jours pendant lesquels vous souhaitez que cette stratégie soit appliquée. Sélectionnez les différents jours (**Sun–Sat**) ou **Everyday**. Entrez une plage d'heures en indiquant l'heure de début (**From**) et l'heure de fin (**To**) ou sélectionnez **24 Hours**.

Paramètres de contrôle d'accès à Internet

Times	Sélectionnez les heures pendant lesquelles vous souhaitez que cette stratégie soit appliquée. Entrez une plage d'heures en indiquant l'heure de début (**From**) et l'heure de fin (**To**) ou sélectionnez **24 Hours**.
Action	
Blocking Everything	Cochez cette case pour bloquer tout le trafic Internet qui répond aux critères spécifiés dans cette page. Désélectionnez-la pour choisir une ou plusieurs des autres options de filtrage.
Blocking by URL and Keyword	Cochez cette case pour empêcher les utilisateurs d'accéder aux URL spécifiées ou aux URL qui contiennent les mots-clés spécifiés. Vous pouvez spécifier jusqu'à quatre URL et jusqu'à six mots-clés.
Blocking by Destination IP Address	Cochez cette case pour empêcher les utilisateurs d'accéder aux adresses IP spécifiées. Vous pouvez spécifier jusqu'à quatre adresses IP.
Blocking by Application	Cochez cette case pour empêcher les utilisateurs d'accéder aux services Internet spécifiés, tels que les services FTP ou Telnet (vous pouvez bloquer jusqu'à trois applications par stratégie). Dans la liste d'applications, cliquez sur l'application que vous souhaitez bloquer. Cliquez ensuite sur le bouton à double flèche droite **(>>)** pour déplacer l'application vers la liste des applications bloquées. Pour supprimer une application de la liste des applications bloquées, cliquez dessus, puis cliquez sur le bouton à double flèche gauche **(<<)**.

Paramètres de contrôle d'accès à Internet

Modify Application	Si l'application que vous souhaitez bloquer n'est pas répertoriée ou si vous souhaitez modifier les paramètres d'un service, spécifiez le nom de l'application dans le champ Application Name. Spécifiez sa plage de ports dans les champs Port Range. Sélectionnez son protocole dans la liste déroulante des protocoles. Cliquez ensuite sur **Add Entry**. Pour modifier un service, sélectionnez-le dans la liste des applications. Modifiez son nom, sa plage de ports et/ou son paramètre de protocole, puis cliquez sur l'icône en forme de stylet **Edit.** Pour supprimer un service, sélectionnez-le dans la liste des applications. Cliquez ensuite sur l'icône **Delete** (x).

Page Advanced Firewall Settings

Utilisez la page Advanced Firewall Settings pour configurer les règles de contrôle d'accès à partir d'Internet (WAN vers LAN).

ÉTAPE 1 Cliquez sur **Network Setup > Firewall > Advanced Firewall Settings**. La fenêtre Advanced Firewall Settings s'ouvre. Cette page vous permet d'ajouter, modifier, consulter et hiérarchiser les règles existantes de la liste des stratégies avancées de pare-feu. Cliquez sur n'importe quelle règle pour afficher des informations détaillées sur la stratégie.

ÉTAPE 2 Pour ajouter une nouvelle règle de pare-feu, cliquez sur **Add Entry**. La fenêtre Advanced Firewall Settings pour la règle s'ouvre

ÉTAPE 3 Spécifiez le nom de la nouvelle règle.

ÉTAPE 4 Cliquez sur **Enabled** pour activer la règle.

ÉTAPE 5 Spécifiez les paramètres d'interface, les informations de port source et de destination, l'action et les informations de planification, tels qu'ils sont définis dans le tableau **Paramètres avancés de pare-feu** ci-dessous.

ÉTAPE 6 Cliquez sur **Submit** pour enregistrer les modifications. La nouvelle règle est ajoutée à la liste des stratégies avancées de pare-feu dans la page des paramètres avancés de pare-feu.

Paramètres avancés de pare-feu

Advanced Firewall Policy List	Répertorie les règles de pare-feu existantes et le nom de stratégie, l'état, l'interface interne et externe et l'état de priorité correspondants de chaque règle. Sélectionnez le niveau de priorité d'une règle dans la liste déroulante Priority pour définir l'ordre dans lequel les règles seront appliquées. La plate-forme SRP utilisera la première règle faisant l'objet d'une correspondance pour déterminer l'action à entreprendre. Une fois terminé, cliquez sur **Submit** pour enregistrer les modifications.
Policy Details	Affiche les informations de stratégie pour la règle sélectionnée.
Rule Name	Spécifiez un nom pour la règle. Vous pouvez spécifier jusqu'à 31 caractères.
Status	Sélectionnez **Enabled** pour activer la règle. La valeur par défaut est Disabled.
IN Interface	Choisissez l'interface WAN entrante **(IN Interface)** pour cette règle, dans la liste déroulante. « ALL WAN » signifie que cette règle est appliquée au trafic entrant sur n'importe quelle interface WAN.
OUT Interface	Choisissez l'interface LAN sortante (**Out Interface**) pour la règle de pare-feu, dans la liste déroulante. « ALL LAN » signifie que cette règle est appliquée au trafic entrant sur n'importe quelle interface LAN.
Source IP Address	Spécifie une adresse IP source à mettre en correspondance.
Source Subnet Mask	Définit le masque générique de l'adresse IP source. Les masques spécifient les bits utilisés et les bits ignorés. Le masque 255.255.255.255 indique que tous les bits sont importants. Le masque 0.0.0.0 indique que tous les bits seront ignorés. Cela signifie que si vous spécifiez une adresse IP de destination, alors que le masque de sous-réseau de destination est défini sur 0.0.0.0, la règle considèrera cette adresse comme une adresse 0.0.0.0/0 (tous).

Paramètres avancés de pare-feu

Destination IP Address	Spécifie une adresse IP de destination à mettre en correspondance.
Destination Subnet Mask	Définit le masque générique de l'adresse IP de destination. Les masques spécifient les bits utilisés et les bits ignorés. Le masque de sous-réseau 255.255.255.255 indique que tous les bits sont importants. Le masque 0.0.0.0 indique que tous les bits seront ignorés. Cela signifie que si vous spécifiez une adresse IP de destination, alors que le masque de sous-réseau de destination est défini sur 0.0.0.0, la règle considèrera cette adresse comme une adresse 0.0.0.0/0 (tous).
Protocol	Spécifiez le protocole pour la règle de pare-feu. Choisissez parmi **TCP**, **UP**, **ICMP** ou **Any**. La valeur par défaut est Any.
Source Port	Choisissez le port TCP/UDP source pour le pare-feu, dans la liste déroulante. La valeur par défaut est « Any », ce qui signifie que le port ne sera pas contrôlé. Choisissez parmi **Single** et **Range** pour définir les ports nécessaires.
Destination Port	Choisissez le port TCP/UDP de destination pour la règle de pare-feu, dans la liste déroulante. La valeur par défaut est « Any ». Choisissez parmi **Single** et **Range** pour définir les ports nécessaires.
Action	Choisissez **Deny** ou **Permit** dans la liste déroulante pour refuser ou autoriser le trafic associé à la règle.
Schedule	Check **Everyday** to apply the firewall rule to all days of the week. Uncheck it to disable it.
Times	Spécifiez les heures pendant lesquelles la règle sera appliquée. La valeur par défaut est de 24 heures. Pour saisir une heure spécifique, sélectionnez **Range** et spécifiez l'heure (au format 24 heures) dans les champs de la plage.

Relais PPPoE

Utilisez la page PPPoE Relay pour définir les paramètres de relais PPPoE. La fonctionnalité de relais PPPoE est à l'écoute du trafic PPP sur les interfaces LAN désignées et les transfère vers le WAN désigné. Les trames reçues sur le WAN sont retransmises par relais au client qui a lancé la session sur le LAN.

ÉTAPE 1 Cliquez sur **Network Setup > PPPoE Relay**. La fenêtre PPPoE Relay s'ouvre. Cette page vous permet de consulter, de modifier ou d'ajouter un nouveau relais.

ÉTAPE 2 Pour ajouter un relais PPPoE, cliquez sur **Add Entry**. La fenêtre PPPoE Relay Add s'ouvre.

ÉTAPE 3 Pour activer le relais PPPoE pour le côté Internet, cliquez sur **Enabled**. La valeur par défaut est Disabled.

ÉTAPE 4 Sélectionnez l'**interface WAN** pour cette règle. Par exemple : WAN1 ou WAN2.

ÉTAPE 5 Sélectionnez l'**interface LAN** pour cette règle. Par exemple : VLAN1 ou VLAN100.

ÉTAPE 6 Cliquez sur **Submit** pour enregistrer les paramètres.

Paramètres de relais PPPoE

WAN interface	Sélectionnez l'**interface WAN** pour cette règle.
LAN interface	Sélectionnez l'**interface LAN** pour cette règle.
PPPoE Relay Status	Permet à un concentrateur d'accès L2TP (LAC, L2TP Access Concentrator) de relayer la fonctionnalité active de détection et de sélection de service pour le protocole PPPoE (PPP over Ethernet) sur un canal de contrôle L2TP (Layer 2 Tunneling Protocol), vers un serveur réseau L2TP (LNS, L2TP Network Server) ou un commutateur de tunnel (nœud à sauts multiples). La fonctionnalité de relais de cette fonction permet au LNS ou au commutateur de tunnel d'annoncer les services qu'il offre au client, offrant ainsi un contrôle de bout en bout des services entre le LNS et un client PPPoE.

DNS dynamique

Utilisez la page Dynamic DNS (DDNS) pour spécifier un service Internet qui permet de localiser des routeurs avec des adresses IP publiques non statiques, en utilisant les noms de domaines Internet. Lorsqu'une nouvelle adresse IP lui est attribuée, la plate-forme SRP met à jour le service DDNS pour garantir que son nom de domaine associé corresponde à cette nouvelle valeur, facilitant ainsi l'accès à distance.

REMARQUE Pour utiliser DDNS, vous devez configurer un compte avec DynDNS.com ou TZO.com.

ÉTAPE 1 Cliquez sur **Network Setup > DDNS**. La fenêtre DDNS s'ouvre.

ÉTAPE 2 Sélectionnez un service DDNS dans la liste déroulante. Sélectionnez **DynDNS.org** ou **TZO.com**. La fenêtre correspondant au service DDNS s'ouvre.

ÉTAPE 3 Spécifiez les informations pour le service que vous avez choisi, telles qu'elles sont définies dans le tableau **Paramètres du service DDNS ci-dessous.**

ÉTAPE 4 Cliquez sur **Submit** pour enregistrer les paramètres.

Paramètres du service DDNS

DDNS Service	Sélectionnez le fournisseur pour votre service DDNS dans la liste déroulante. Sélectionnez **DynDNS.org** ou **TZO.com**. Le service DDNS est désactivé par défaut. **REMARQUE** Vous devez souscrire un compte auprès de l'un de ces fournisseurs avant de pouvoir utiliser ce service.
Paramètres DynDNS.org	
User Name	Spécifiez le nom d'utilisateur de DynDNS.org.
Password	Spécifiez le mot de passe de DynDNS.org.
Host Name	Spécifiez votre nom d'hôte. Par exemple : nom.dyndns.org.
System	Sélectionnez le service DynDNS que vous utilisez. Choisissez **Dynamic**, **Static** ou **Custom**.

Paramètres du service DDNS

Mail Exchange (facultatif)	Spécifiez l'adresse de votre serveur Mail Exchange, de sorte que les courriers électroniques destinés à votre adresse DynDNS aillent directement vers votre serveur de messagerie.
Mail Exchange (Backup MX)	Permet au serveur Mail Exchange d'être utilisé comme serveur de secours. Pour activer cette fonctionnalité, sélectionnez **Enabled**. Si vous n'êtes pas sûr du paramètre à utiliser, conservez le paramètre par défaut, **Disabled**.
Wildcard	Vous permet d'utiliser un caractère générique dans l'adresse DDNS. Par exemple, si votre adresse DDNS est myplace.dyndns.org et que vous activez le caractère générique, vous pouvez également utiliser x.myplace.dyndns.org, où x correspond au caractère générique. Pour activer les caractères génériques, sélectionnez **Enabled**. Si vous n'avez pas souscrit à ce service, ou ne savez pas, conservez le paramètre par défaut, Disabled.
Internet IP Address	Affiche votre adresse IP actuelle.
Status	Affiche votre état DDNS.
Update	Pour déclencher manuellement une mise à jour, cliquez sur le bouton **Update**.
Paramètres TZO.org	
E-mail Address	Spécifiez l'adresse e-mail de votre compte TZO.
TZO Key	Spécifiez la clé de votre compte TZO.
Domain Name	Spécifiez votre nom d'hôte. Par exemple : nom.dyndns.org.
Internet IP Address	Affiche votre adresse IP actuelle.
Status	Affiche votre état DDNS.
Update	Pour déclencher manuellement une mise à jour, cliquez sur le bouton **Update**.

Configuration DMZ

Utilisez les pages DMZ (Demilarized Zone) pour configurer un accès externe complet aux serveurs locaux qui exécutent les services Internet. La plate-forme SRP propose deux types de configuration DMZ : une zone DMZ logicielle (ou hébergée), qui mappe le trafic pour une adresse publique à un hôte local adressé de façon privée, ou une zone DMZ matérielle, qui utilise une interface/un réseau dédié(e) de couche 2 pour que les hôtes DMZ optimisent la protection pour les clients LAN privés.

Pour accéder à ces pages, cliquez sur **Network Setup > DMZ** dans l'utilitaire de configuration.

Page Software DMZ

ÉTAPE 1 Cliquez sur **Network Setup > DMZ > Software DMZ**. La fenêtre Software DMZ s'ouvre. Cette page vous permet de visualiser toutes les zones DMZ logicielles actuellement installées, de consulter l'état DMZ, de modifier une zone DMZ et d'ajouter une zone DMZ.

ÉTAPE 2 Pour ajouter une zone DMZ logicielle, cliquez sur **Add Entry.** La fenêtre DMZ Setting correspondant à la nouvelle zone DMZ s'ouvre.

ÉTAPE 3 La zone DMZ logicielle est activée par défaut à sa création. Pour la désactiver, sélectionnez **Disable**.

ÉTAPE 4 Spécifiez les paramètres de la zone DMZ, tels qu'ils sont définis dans le tableau **Paramètres de la zone DMZ logicielle** ci-dessous.

ÉTAPE 5 Cliquez sur **Submit** pour enregistrer les paramètres.

Paramètres de la zone DMZ logicielle

Status	La zone DMZ logicielle est activée par défaut. Pour la désactiver, sélectionnez **Disable**.
Public IP	Spécifiez l'adresse **IP publique** que ce serveur DMZ exposera à Internet.
Private IP	Spécifiez l'adresse **IP privée**. Il s'agit de l'adresse IP privée du serveur sur le LAN, qui correspond à l'adresse IP publique.
WAN Interface	Sélectionnez un type d'**interface WAN** dans la liste déroulante. Il s'agit de l'interface WAN à la laquelle cette zone DMZ correspondante se liera.

Page Hardware DMZ

Utilisez la page Hardware DMZ pour configurer le port LAN 4 pour l'accès public aux serveurs Web et autres du client, qui sont accessibles à partir d'Internet. Les autres ports réseau LAN sur la plate-forme continueront d'être utilisés pour le trafic interne privé.

REMARQUE Cette fonctionnalité peut uniquement être utilisée avec les interfaces WAN encapsulées Ethernet (c'est-à-dire, Ethernet ou EoA), et les interfaces WAN PPP, PPTP, L2TP ou IPoA ne peuvent pas être utilisées.

ÉTAPE 1 Cliquez sur **Network Setup > DMZ > Hardware DMZ**. La fenêtre Hardware DMZ s'ouvre. Cette page vous permet d'activer la fonctionnalité de zone DMZ matérielle et d'ajouter, consulter ou modifier les adresses publiques qui seront transmises à la zone DMZ matérielle.

Cliquez sur **Add Entry** pour créer des adresses IP publiques qui seront transférés vers la zone DMZ. La page DMZ Setting correspondant à la nouvelle zone DMZ matérielle s'affiche.

REMARQUE La fonctionnalité de zone DMZ matérielle elle-même est désactivée par défaut. Les entrées d'adresse individuelles sont activées par défaut à leur création.

ÉTAPE 2 Cliquez sur **Submit** pour enregistrer les paramètres.

Paramètres de zone DMZ matérielle

Status	Les entrées DMZ sont activées par défaut. Lorsque cette option est activée, le port LAN 4 agit en tant que port DMZ. Lorsque l'option est désactivée, le port agit en tant que port LAN normal pour le trafic interne privé et la fonctionnalité de zone DMZ matérielle est désactivée.
Public IP	Spécifiez une adresse **IP publique** équivalente à l'adresse IP du serveur qui se trouve derrière le port de la zone DMZ matérielle.
WAN interface	Dans la liste déroulante d'interface WAN, choisissez l'**interface WAN** avec laquelle cette adresse se liera.

Protocole de gestion des groupes Internet (IGMP)

Utilisez la page IGMP pour configurer les paramètres pour le protocole IGMP (Internet Group Management Protocol). Le protocole IGMP est un protocole de signalisation qui prend en charge la multidiffusion IP pour IPTV. Par exemple, utilisez le protocole IGMP si vous bénéficiez de la télévision IP (IPTV) avec plusieurs zones de configuration sur le même réseau local, qui ont des flux vidéo différents, exécutés simultanément.

ÉTAPE 1 Cliquez sur **Network Setup > IGMP**. La fenêtre IGMP s'ouvre.

ÉTAPE 2 Pour permettre au trafic multidiffusion de traverser la plate-forme SRP pour vos périphériques d'application multimédia, utilisez le paramètre par défaut, **Enabled**.

ÉTAPE 3 Sélectionnez la version que vous voulez prendre en charge, **IGMP v1** ou **IGMP v2**. Si vous n'êtes pas sûr de la version à sélectionner, utilisez le paramètre par défaut, IGMP v2.

ÉTAPE 4 Choisissez l'**interface WAN** à laquelle le service IGMP se liera (Auto, Ether_WAN1, USB_3G ou Ether_WAN2).

ÉTAPE 5 Activez **Immediate Leave** si vous utilisez des applications IPTV et souhaitez autoriser la commutation ou la rotation des chaînes sans retard ni délai. Sinon, conservez le paramètre par défaut, Disabled.

ÉTAPE 6 Cliquez sur **Submit** pour enregistrer les paramètres.

Paramètres IGMP

Proxy IGMP	Pour activer le proxy IGMP, sélectionnez **Enabled**. Cela permet au trafic multidiffusion de traverser la plate-forme SRP pour les périphériques d'application multimédia.
Support IGMP Version	Sélectionnez la version IGMP dans la liste déroulante. Sélectionnez **IGMP v1** ou **IGMP v2**. Si vous n'êtes pas sûr de la version à sélectionner, conservez le paramètre par défaut, IGMP v2.
WAN Interface	Choisissez l'**interface WAN** à laquelle le service IGMP se liera. Le service IGMP peut prendre en charge une seule interface WAN dédiée à la fois. Le paramètre AUTO par défaut permet à la plate-forme SRP de suivre l'itinéraire système par défaut actuel pour le transfert multidiffusion.

Paramètres IGMP

Immediate Leave	Sélectionnez **Enabled** si vous utilisez des applications IPTV et si vous souhaitez autoriser la commutation ou la rotation des chaînes sans retard ni délai. Sinon, conservez le paramètre par défaut, Disabled.

Universal Plug and Play

Utilisez la page UPnP pour activer le protocole UPnP. Le protocole UPnP (Universal Plug and Play) permet aux périphériques locaux de détecter la plate-forme SRP afin de contrôler certaines configurations.

ÉTAPE 1 Cliquez sur **Network Setup > UPnP**. La fenêtre UPnP s'ouvre.

ÉTAPE 2 Le protocole UPnP est activé par défaut. Pour la désactiver, sélectionnez **Disable**.

ÉTAPE 3 Configurez les paramètres UPnP tels qu'ils sont définis dans le tableau **Paramètres UPnP** ci-dessous.

ÉTAPE 4 Cliquez sur **Submit** pour enregistrer les paramètres.

Paramètres UPnP

UPnP	Le protocole UPnP est activé par défaut. Pour la désactiver, sélectionnez **Disable**.
Allow Users to Configure	Lorsque cette option est activée (par défaut), les clients locaux peuvent utiliser le protocole UPnP pour modifier la configuration et le comportement de la plate-forme SRP. Si vous souhaitez uniquement permettre aux clients de détecter la plate-forme SRP à l'aide du protocole UPnP, sélectionnez **Disabled**.
Keep UPnP Configurations After System Reboot	Lorsque cette option est activée, la plate-forme SRP enregistre les modifications de configuration apportées par les clients après un redémarrage du système. La valeur par défaut est Disabled.

Cisco Discovery Protocol

Utilisez la page CDP pour spécifier les paramètres CDP (Cisco Discovery Protocol) sur votre réseau. Le protocole CDP est un protocole de détection de périphérique au niveau de la liaison, disponible sur de nombreux produits Cisco. Chaque périphérique prenant en charge le protocole CDP envoie des messages périodiques à une adresse de multidiffusion et est également à l'écoute des messages périodiques envoyés par les autres pour s'informer sur les périphériques voisins.

ÉTAPE 1 Cliquez sur **Network Setup > CDP Setting**. La fenêtre CDP Setting s'ouvre.

Vous pouvez choisir d'activer le protocole CDP sur certaines, l'ensemble ou aucune des interfaces Ethernet de la plate-forme SRP. Nous vous recommandons d'utiliser le paramètre par défaut, Per Port, qui active le protocole CDP sur les ports LAN uniquement. L'activation du protocole CDP n'est pas recommandée sur le port WAN, car il est connecté à un réseau non sécurisé.

ÉTAPE 2 Spécifiez les valeurs du minuteur CDP (CDP Timer) et la participation des ports, telles qu'elles sont définies dans le tableau **Cisco Discovery Protocol ci-dessous.**

ÉTAPE 3 Cliquez sur **Submit** pour enregistrer les paramètres.

Paramètres CDP

CDP	Active ou désactive le protocole CDP. Vous pouvez choisir d'activer le protocole CDP sur certaines, l'ensemble ou aucune des interfaces Ethernet de la plate-forme SRP. CDP per port est le paramètre par défaut (recommandé).
CDP Timer	Spécifiez l'intervalle auquel les paquets CDP successifs peuvent être envoyés. Spécifiez une valeur comprise entre 5 et 900 secondes. La valeur par défaut est 60 secondes.

Paramètres CDP

CDP Hold Timer	Utilisez le paramètre CDP Hold Timer pour spécifier la durée pendant laquelle le périphérique de réception doit conserver un paquet CDP (Cisco Discovery Protocol) provenant de votre routeur avant de le supprimer. Spécifiez une valeur comprise entre 10 et 255 secondes. La valeur par défaut est de 80 secondes et doit être définie sur une valeur supérieure à celle du minuteur de transmission CDP.
Interface List	Cochez la case **Enable** pour sélectionner les interfaces qui exécuteront le protocole CDP.

Réseau invité

Utilisez les pages de paramètres de réseau invité pour configurer un réseau invité sur la plate-forme SRP. Un réseau invité permet aux utilisateurs de se connecter en toute sécurité à Internet sans accéder à votre réseau privé.

Cette section comprend les rubriques suivantes :

- **Page Basic Configuration**
- **Page User Account**
- **Personnalisation de la page d'accueil**

Page Basic Configuration

Utilisez la page Basic Configuration pour configurer les paramètres réseau pour le réseau invité.

Avant de configurer le réseau invité, procédez comme suit :

Activez le réseau sans fil. Le réseau sans fil est désactivé par défaut. Pour l'activer, accédez à la page **Interface Setup > Wi-Fi Settings > Basic Wireless Settings** et configurez les paramètres de sécurité pour l'accès privé. Nous vous recommandons d'utiliser la sécurité WPA2 avec le cryptage AES, car il est plus sécurisé et moins vulnérable aux attaques. Pour obtenir des informations sur la configuration, reportez-vous à **Page Basic Wireless Settings, page 65**.

- Vérifiez que SSID3 n'est pas utilisé. Lorsque le réseau invité est activé, SSID3 est automatiquement associé au VLAN du réseau invité. Si SSID3 est en cours d'utilisation, vous devez le réaffecter à un autre SSID.

ÉTAPE 1 Cliquez sur **Network Setup > Guest Network > Basic Configuration**. La fenêtre Basic Configuration s'ouvre.

La première fois que vous configurez le réseau invité, une vérification préalable est effectuée pour vérifier que toutes les conditions sont remplies pour créer un réseau invité. Avant de continuer, veillez à effectuer une sauvegarde de votre configuration actuelle, puis cliquez sur **Yes** pour continuer.

ÉTAPE 2 Sélectionnez **Enabled** pour activer le réseau invité. La valeur par défaut est Disabled.

ÉTAPE 3 Spécifiez les paramètres réseau tels qu'ils sont définis dans le tableau **Configuration de base du réseau invité ci-dessous.**

ÉTAPE 4 Cliquez sur **Submit** pour enregistrer les paramètres.

.

Configuration de base du réseau invité

Feature	Cliquez sur **Enabled** pour créer un réseau invité. La valeur par défaut est Disabled.
Network	Spécifiez l'adresse de sous-réseau du réseau invité.
Default Lease Time	Spécifiez la durée (paramètre global) pendant laquelle l'utilisateur peut être connecté au réseau invité. La plage s'étend de 1 à 168 heures. La valeur par défaut est de 24 heures.
Start lease from	Spécifiez l'heure à laquelle le bail commence. Vous pouvez choisir le moment où l'invité se connecte pour la première fois (**First Login**) ou le moment où le compte invité est créé pour la première fois (**Account Creation**).
Auto Redirect URL	Cliquez sur **Enabled** pour rediriger automatiquement l'invité vers l'URL spécifiée dans le champ Redirect URL (champ ci-dessous).
Redirect URL	Spécifiez l'URL de la page Web que le client voit initialement lorsqu'il se connecte au réseau invité, comme, par exemple, la page d'accueil de sa société.

Page User Account

Utilisez la page User Account pour configurer un compte d'utilisateur de réseau invité sur la plate-forme SRP. Vous pouvez configurer jusqu'à 50 comptes d'utilisateur invité, chaque utilisateur étant en mesure de connecter jusqu'à trois périphériques à l'aide d'un compte unique.

Le nombre maximal de sessions invité actives dépend du modèle de plate-forme SRP. Les modèles SRP520W-U permettent d'associer jusqu'à 25 périphériques invité à tout moment. Les modèles SRP540W prennent en charge jusqu'à 50 périphériques simultanés.

ÉTAPE 1 Cliquez sur **Network Setup > Guest Network > User Account**. La fenêtre User Account s'ouvre.

Cette page vous permet d'ajouter un nouveau compte invité, de modifier ou supprimer un compte, ou d'exporter la liste de vos comptes existants vers un fichier texte.

ÉTAPE 2 Pour ajouter un compte invité, cliquez sur **Add Account**. La fenêtre Guest Network Account s'ouvre.

ÉTAPE 3 Spécifiez les paramètres de compte invité, tels qu'ils sont définis dans le tableau **Compte d'utilisateur du réseau invité ci-dessous.**

ÉTAPE 4 Cliquez sur **Submit** pour enregistrer les modifications.

Compte d'utilisateur du réseau invité

Account	Spécifiez un nom pour le compte invité. Ce nom est sensible à la casse et peut contenir uniquement des lettres, des chiffres, « @ », ou « . »
Password	Cliquez sur le bouton **Generate** pour créer un mot de passe pour cet utilisateur. Le mot de passe qui doit être généré est un mot de passe numérique à 6 chiffres. Vous pouvez modifier le compte pour générer un nouveau mot de passe, si nécessaire.

Compte d'utilisateur du réseau invité

Lease Time	Spécifiez la durée pendant laquelle l'utilisateur peut accéder à Internet via le réseau invité. Pour spécifier une autre durée, cliquez sur **Other**. La plage s'étend de 1 à 168 heures. **REMARQUE :** Une fois la durée de bail expirée, le compte d'utilisateur est supprimé et tous les périphériques associés sont supprimés du réseau sans fil.
Export Account List	Cliquez sur ce bouton pour enregistrer les comptes invité et les mots de passe dans un fichier texte.

Personnalisation de la page d'accueil

Vous pouvez personnaliser la page de connexion d'un utilisateur dans une langue quelconque, en configurant la page d'accueil du portail du réseau invité.

ÉTAPE 1 Cliquez sur **Network Setup > Guest Network > Welcome Page.** La fenêtre Welcome Page s'ouvre.

Spécifiez les paramètres de la page d'accueil, tels qu'ils sont définis dans le tableau **Page d'accueil du réseau invité ci-dessous. C'est la page que l'utilisateur verra lorsqu'il se connectera au réseau invité.**

ÉTAPE 2 Une fois terminé, cliquez sur **Submit** pour enregistrer les modifications.

Lorsque l'utilisateur se connecte à sa page d'accueil, sa page d'accueil personnalisée s'ouvre.

- Si l'option Auto Redirect URL est activée, le navigateur de l'invité est dirigé vers l'URL spécifiée dans la fenêtre Basic Configuration Settings.
- Si l'option Auto Direct URL est désactivée, la fenêtre Guest Network Login Information s'ouvre et affiche le nom d'utilisateur invité et la durée de bail restante.

Page d'accueil du réseau invité

Company Title	Nom de la société qui apparaît sur la gauche de la page de connexion utilisateur au réseau invité.
Welcome Title	Message de bienvenue qui apparaît sur la gauche de la page de connexion utilisateur au réseau invité.
Username Title	Étiquette du champ de nom d'utilisateur qui apparaît sur le côté droit de la page de connexion au réseau invité. Le titre par défaut est Username.
Password Title	Étiquette du champ de mot de passe qui apparaît sur le côté droit de la page de connexion au réseau invité. Le titre par défaut est Password.
Login Button Title	Intitulé du bouton qui apparaît dans la page de connexion au réseau invité et qui permet de se connecter au réseau invité. Le titre par défaut est Login.
Agree Title	Texte d'acceptation utilisé dans l'avis de déclaration qui apparaît dans la page de connexion au réseau invité. Le texte par défaut est « I agree to the conditions of use ».
Logout Info Title	Titre descriptif de la page de déconnexion du réseau invité.
Logout Button Title	Intitulé du bouton qui apparaît dans la page des informations de connexion au réseau invité et qui permet de se déconnecter du réseau invité. Le titre par défaut est Logout.
Time Left Title	Indique le temps restant dont dispose l'utilisateur sur le réseau invité avant d'être déconnecté (apparaît dans la page des informations de connexion au réseau invité).
Copyright	Mention de droits d'auteur qui s'affiche en bas à gauche de la page de connexion au réseau invité.
Title Font Color	Couleur de police qui figure dans les pages de connexion et de déconnexion du réseau invité. Sélectionnez le blanc (**White**) ou le noir (**Black**).
Error 1, Error 2 and Error 3	Messages qui s'affichent sur le réseau invité en cas d'erreur. Pour modifier un message, saisissez le nouveau texte dans le champ d'erreur approprié, puis cliquez sur **Submit**.

Page d'accueil du réseau invité

Upload Files	Vous permet de charger et modifier l'image d'arrière-plan et le logo qui apparaissent dans la page de connexion au réseau invité. Seuls des fichiers images JPEG ou GIF sont autorisés. La taille de fichier maximale de l'image d'arrière-plan est de 256 Ko. La taille maximale du logo est de 10 Ko. Cliquez sur **Browse** pour localiser le fichier, puis cliquez sur **Upload** pour ajouter la nouvelle image. **REMARQUE** Si vous téléchargez un fichier graphique, l'état de l'image passe de Default à Customize.
Declaration	Cliquez sur **Enabled** pour afficher la déclaration (juridique) et la case à cocher d'acceptation dans la page de connexion au réseau invité. La valeur par défaut est Disabled. Lorsque cette option est activée, la déclaration apparaît dans la zone de texte déroulante située au-dessous. Pour ajouter un retour chariot au texte, utilisez la balise HTML . Par exemple : aaabr >bbbb

Usurpation d'adresse DNS

Utilisez la page DNS Spoofing pour configurer le service d'usurpation d'adresse DNS sur la plate-forme SRP. L'usurpation d'adresse DNS est un service qui complète la fonctionnalité de proxy DNS, en permettant à la plate-forme SRP d'intercepter les requêtes DNS provenant des clients locaux et de répondre directement en utilisant le nom d'hôte configuré localement pour résoudre les informations de mappage.

ÉTAPE 1 Cliquez sur Network Setup > DNS Spoofing. La fenêtre DNS Spoofing s'ouvre. Cette fenêtre vous permet de consulter les entrées existantes dans la liste d'usurpation d'adresse DNS et d'ajouter une nouvelle entrée d'usurpation d'adresse DNS.

ÉTAPE 2 Cliquez sur **Enabled** pour activer l'usurpation d'adresse DNS.

ÉTAPE 3 Pour ajouter une nouvelle entrée, cliquez sur **Add Entry**. La fenêtre DNS Spoofing Add s'ouvre.

ÉTAPE 4 Spécifiez le nom d'hôte et l'adresse IP.

ÉTAPE 5 Cliquez sur **Submit** pour enregistrer les modifications.

6

Configuration de la voix

Ce chapitre décrit comment configurer les paramètres vocaux et les services voix pour les plates-formes prêtes pour les services. Il comprend les sections suivantes :

- **Configuration des Services Voix**
- **Configuration des paramètres de voix**

Configuration des Services Voix

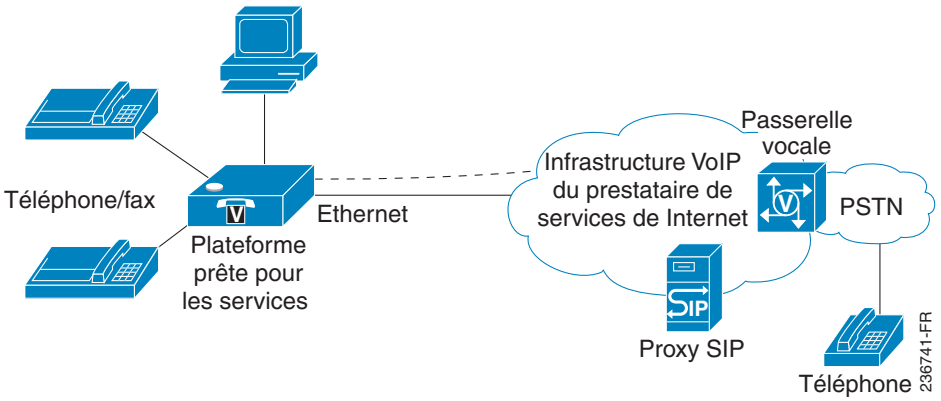
Cette section explique comment configurer votre SRP afin de répondre aux exigences des clients en matière de services voix. Elle comprend les rubriques suivantes :

- **Fonctionnement des ports voix**
- **Gestion des services d'identification de l'appelant**
- **Configuration des plans de numérotation**
- **Implémentation d'appel sécurisé**

Fonctionnement des ports voix

La SRP a un certain nombre de ports voix qui permettent de passer des appels à partir des combinés ou des télécopieurs analogiques connectés localement, à l'aide des services de téléphonie Internet SIP. Outre les ports (FXS) du combiné, la SRP dispose également d'un port de ligne unique (FXO) qui peut être utilisé pour passer des appels vers le réseau téléphonique en cas de défaillance du haut débit ou même de la SRP.

Le port FXO de la SRP est principalement utilisé comme sauvegarde si une défaillance d'inscription se produit, si le réseau est déconnecté ou si l'alimentation de la SRP est en panne. Les appels ne peuvent pas être acheminés dynamiquement à cette interface dans des conditions de fonctionnement normal pour les modèles SRP520, mais ils peuvent l'être pour les modèles SRP540. Reportez-vous aux paramètres sur la page **Voice > PSTN**.



La SRP conserve l'état de chaque appel passé via l'interface FXS et réagit de manière appropriée aux événements produits par l'utilisateur (tels qu'un raccroché/décroché ou un crochet commutateur). Étant donné que la SRP utilise le protocole SIP (Session Initiation Protocol), elle est compatible avec la plupart des offres des fournisseurs d'accès à Internet.

Fonctionnalités voix de la SRP

La SRP est fournie avec des ports voix programmables et riches en fonctionnalités, pouvant être personnalisés grâce à un large éventail de paramètres de configuration. Les sections suivantes décrivent les facteurs qui contribuent à la qualité vocale :

- **Codecs pris en charge**
- **Redondance du proxy SIP**
- **Autres fonctionnalités voix de la SRP**

Codecs pris en charge

Les ports voix de la SRP prennent en charge les codecs suivants :

Codec	Description
G.711 (A-law et mu-law)	Codecs de très faible complexité qui prennent en charge les transmissions voix numérisées non compressées de 64 Kbits/s de une à dix trames vocales de 5 ms par paquet. Ces codecs procure la plus haute qualité vocale à bande étroite la plus élevée et utilise la plupart des bandes passantes des codecs disponibles.

G.726-32	Codec de faible complexité qui prend en charge la transmission voix numérisée compressée de 32 Kbits/s de une à dix trames vocales de 10 ms par paquet. Ce codec procure une haute qualité vocale.
G.729a	Algorithme de codage audio ITU G.729 utilisé pour compresser la parole numérisée. G.729a est une version simplifiée de G.729 nécessitant environ la moitié de la puissance de traitement de G.729. Les transmissions binaires G.729 et G.729a sont compatibles et interopérables, mais ne sont pas identiques.

L'administrateur peut sélectionner les codecs préférés à utiliser pour chaque ligne. Voir aussi **Configuration audio, page 210**.

En outre, la négociation pour un codec voix optimal dépend parfois de la capacité d'un périphérique à faire correspondre un nom de codec avec le codec utilisé par un périphérique distant. Vous pouvez nommer les différents codecs individuellement, de sorte que la SRP puisse négocier avec succès le codec avec l'équipement distant. Pour obtenir plus d'informations, reportez-vous à la section **Configuration audio, page 210**.

Redondance du proxy SIP

Dans les déploiements standard de téléphonie IP commerciale, tous les appels sont établis via un serveur proxy SIP. Un serveur proxy SIP classique peut prendre en charge des milliers d'abonnés. Il est important qu'un serveur de sauvegarde soit disponible afin qu'un serveur actif puisse être commuté temporairement pour la maintenance. La SRP prend en charge l'utilisation de serveurs proxy SIP de secours (via l'enregistrement SRV DNS), afin de réduire les interruptions de service.

Configurer votre serveur DNS avec une liste d'adresses de proxy SIP constitue une façon simple de prendre en charge la redondance de proxy. La SRP peut être invitée à contacter un serveur proxy SIP dans un domaine nommé dans le message SIP. La SRP consulte le serveur DNS pour obtenir la liste des hôtes dans un domaine donné proposant les services SIP. Si une entrée existe, le serveur DNS renvoie un enregistrement SRV contenant la liste des serveurs proxy SIP pour le domaine, avec leur nom d'hôte, la priorité, les ports d'écoute, etc. La SRP tente de contacter la liste des hôtes dans l'ordre de leur priorité établie.

Si la SRP utilise actuellement un serveur proxy de faible priorité, elle teste périodiquement le proxy de plus haute priorité afin de déterminer s'il est de nouveau en ligne et bascule sur ce proxy de plus haute priorité dès que possible. La redondance de proxy SIP est configurée dans les pages Line (1 à 4) dans l'utilitaire de configuration des plate-formes prêtes pour les services. Voir aussi **Pages Line (1-4), page 194**.

Autres fonctionnalités voix de la SRP

Le tableau suivant résume les autres fonctionnalités voix proposées par la SRP.

Fonctionnalité	Description
Silence Suppression	La détection d'activité vocale (VAD) avec suppression des silences est un moyen d'augmenter le nombre d'appels pris en charge par le réseau en réduisant la bande passante moyenne requise pour un seul appel. La détection d'activité vocale utilise un algorithme avancé pour distinguer entre les signaux verbaux et non-verbaux. En fonction des statistiques actuelles et anciennes, l'algorithme de détection d'activité vocale détermine si la parole est présente ou non. Lorsque l'algorithme de détection d'activité vocale détermine qu'il n'y a pas d'activité, la suppression de silences et les services CNG (Comfort Noise Generation) sont activés. Cela est rendu possible en éliminant et en ne transmettant pas le silence naturel qui est généré dans une connexion bidirectionnelle normale. La bande passante IP est utilisée uniquement lorsqu'une personne parle. Pendant les périodes de silence d'un appel téléphonique, une bande passante supplémentaire est disponible pour d'autres appels vocaux ou pour le trafic de données car les paquets de silence ne sont pas transmis sur le réseau. Les services CNG (Comfort Noise Generation) fournissent un bruit blanc (sons) de fond généré artificiellement, conçu pour indiquer aux appelants que leur appel est toujours en cours pendant les périodes de silence. Lorsque les services CNG (Comfort Noise Generation) ne sont pas utilisés, l'appelant pourrait croire que son appel a été interrompu à cause des périodes de « silence absolu » créées par la détection d'activité vocale et la fonction de suppression des silences.

Fonctionnalité	Description
Modem and Fax Pass-Through	Le mode Pass-through du modem ne peut être déclenché qu'en composant le numéro défini à l'avance dans le Modem Line Toggle Code. Voir aussi **Page Regional, page 173**. **FAX pass-through mode** est déclenché par la détection d'une tonalité CED/CNG ou d'un événement NSE. **Echo canceller** est automatiquement désactivé pour le mode Modem permettant le trafic via un port voix. **Echo canceller** est désactivé pour le mode Télécopie permettant le trafic via un port voix si le paramètre FAX Disable ECAN (Ligne 1 ou onglet 2) est défini sur « yes » pour cette ligne (dans ce cas le mode Télécopie permettant le trafic via un port voix est identique au mode Modem permettant le trafic via un port voix). **Call waiting and silence suppression** est automatiquement désactivé pour les modes Modem permettant le trafic via un port voix et Télécopie permettant le trafic via un port voix. En outre, la transmission DTMF hors-bande est désactivée pendant le mode Télécopie permettant le trafic via un port voix ou le mode Modem permettant le trafic via un port voix.

Fonctionnalité	Description
Adaptive Jitter Buffer	La SRP mettre en mémoire tampon les paquets voix entrants pour réduire l'impact des délais réseau variables. Ce traitement est appelé mise en tampon d'instabilité. La taille du tampon d'instabilité s'adapte de manière réactive aux conditions évolutives du réseau. La SRP comprend un paramètre de contrôle du niveau d'instabilité du réseau pour chaque ligne de service. Le niveau d'instabilité détermine l'agressivité avec laquelle la SRP tente de réduire le tampon d'instabilité progressivement, afin de diminuer le retard global. Si le niveau d'instabilité est élevé, il restreint le tampon plus progressivement. Si le niveau d'instabilité est faible, il le restreint plus rapidement. Le tampon d'instabilité adaptable est configuré dans les pages Line. Voir aussi **Pages Line (1-4), page 194**.
International Caller ID Delivery	Outre la prise en charge des méthodes Bellcore (FSK) et Swedish/Danish (DTMF) pour la remise de l'identification de l'appelant (CID), la SRP procure un important sous-réseau de méthodes conformes ETSI permettant de prendre en charge l'équipement CID international. Le CID international est configuré à partir de la page PSTN. Voir aussi **Page PSTN (modèles SRP540 uniquement), page 217**.
Secure Calls	Un utilisateur (s'il est autorisé par le prestataire de services ou l'administrateur) a l'option d'effectuer un appel securisé vers l'extérieur dans le sens où les paquets audio sont cryptés dans les deux directions.
Adjustable Audio Frames Per Packet	Cette fonctionnalité permet à l'utilisateur de définir le nombre de trames audio contenues dans un paquet RTP. Ils peuvent contenir entre 1 et 10 trames audio. L'augmentation du nombre de paquets réduit la bande passante utilisée, mais elle augmente aussi le délai et peut affecter la qualité vocale. Les paquets RTP sont configurés sur la page SIP. Voir aussi **Page SIP, page 156.**

Fonctionnalité	Description
Relais DTMF	La SRP peut relayer des chiffres DTMF en tant qu'événements hors bande afin de préserver la fidélité de ces chiffres. Cette opération permet d'améliorer la fiabilité de la transmission DTMF requise par de nombreuses applications de réponse vocale interactive, telles que les services bancaires à numéro composé et les informations de compagnies aériennes. Le relais DTMF est configuré dans le paramètre DTMF Tx Mode, sur les pages Line. Voir aussi **Pages Line (1-4), page 194**.
Call Progress Tones	Les tonalités de progression d'appel de la SRP sont configurables. Elles sont générées localement sur la SRP, afin que l'utilisateur final soit informé de l'état (comme la tonalité de retour). Les paramètres pour chaque type de tonalité (par exemple une tonalité de retour à un utilisateur final) peuvent inclure la fréquence et l'amplitude de chaque composant et les informations indiquant la cadence. Les tonalités de progression d'appel sont configurées dans la page Regional. Reportez-vous à la section **Page Regional, page 173**.
Call Progress Tone Pass Through	Cette fonctionnalité permet à l'utilisateur d'entendre les tonalités de progression de l'appel (telle qu'une sonnerie) qui est générée par un réseau éloigné.
Echo Cancellation	Un conflit d'impédance entre le téléphone et le port de la passerelle de téléphonie IP peut créer un écho rapproché. La SRP comporte un suppresseur d'écho rapproché qui compense la correspondance d'impédance. La SRP implémente également un suppresseur d'écho avec un générateur de confort de bruit (CNG), afin que l'écho résiduel soit imperceptible. La suppression de l'écho est configurée à partir des pages Line. Voir aussi **Pages Line (1-4), page 194.**

Fonctionnalité	Description
Signaling Hook Flash Event	La SRP peut signaler des événements de crochet commutateur au proxy au cours d'un appel connecté. Cette fonctionnalité peut être utilisée pour procurer des services avancés en cours d'appel avec un contrôle d'appel de tiers. Selon les fonctionnalités offertes par le prestataire de services utilisant le contrôle d'appel de tiers, les fonctionnalités ATA suivantes peuvent être désactivées pour signaler correctement un événement d'actionnement du crochet commutateur au commutateur logiciel : **Service d'appel en attente** : fait référence au paramètre call waiting serv des pages Line) **Service de conférence à trois** : fait référence au paramètre three-way conf serv des pages Line) **Service d'appel à trois** : fait référence au paramètre three-way call serv des pages Line) Vous pouvez configurer la durée autorisée pour la détection d'un crochet commutateur à l'aide du paramètre Hook Flash Timer sur la page Regional. Voir aussi **Page Regional, page 173**.
Configurable Dial Plan with Interdigit Timers	La SRP comporte trois minuteurs inter-chiffres configurables : **Initial timeout (T)** : signale que le combiné est décroché le combiné et qu'aucun chiffre n'a encore été composé. **Long timeout (L)** : signale la fin de la chaîne de composition ; cela signifie qu'aucun autre chiffre n'est attendu. **Short timeout (S)** : utilisé entre les chiffres ; c'est-à-dire qu'après la composition d'un chiffre, un bref instant évite que ce chiffre ne soit reconnu une seconde fois. Pour de plus amples informations, reportez-vous à la section **Configuration des plans de numérotation, page 137.**

Fonctionnalité	Description
Polarity Control	La SRP permet la définition de la polarité lorsqu'un appel est connecté et lorsqu'un appel est déconnecté. Cette fonctionnalité est nécessaire pour prendre en charge certains systèmes de téléphone payant et les répondeurs. Le contrôle de polarité est configuré dans les pages Line. Voir aussi **Pages Line (1-4), page 194**.
Calling Party Control	Le contrôle de l'appelant (CPC) signale à l'appareil de l'appelé que l'appelant a raccroché au cours d'un appel connecté en retirant momentanément la tension entre la pointe et l'anneau. Cette fonctionnalité est utile pour les répondeurs, qui connaissent ainsi le moment de se désengager. La fonctionnalité CPC est configurée dans la page Regional. Reportez-vous au **Page Regional, page 173.**
Report Generation and Event Logging	La SRP enregistre divers états et rapports d'erreur pour aider les fournisseurs d'accès à diagnostiquer les problèmes et à évaluer les performances de leurs services. Les informations peuvent être interrogées par un agent autorisé, utilisant HTTP avec une authentification Digest, par exemple. Les informations peuvent être organisées sous la forme d'une page XML ou d'une page HTML. La génération de rapports et la consignation des événements sont configurées à partir de la page System. Voir aussi **Page System, page 155.**

Fonctionnalité	Description
Syslog and Debug Server Records	Les enregistrements serveur Syslog et de débogage sont plus détaillées que la génération de rapports et la consignation des événements. En utilisant les paramètres de configuration, la SRP vous permet de sélectionner le type d'activité/ événements qui doit être consigné. Les archives serveur syslog et débogage permettent de capturer les informations à envoyer au serveur Syslog. Les enregistrements serveur Syslog et de débogage sont configurées à partir de la page System. Reportez-vous au **Page System, page 155.**
SIP Over TLS	La SRP permet l'utilisation du SIP sur Transport Layer Security (TLS). SIP sur TLS est conçu pour éliminer la possibilité d'activité malveillante en cryptant les messages SIP entre le fournisseur d'accès et l'utilisateur final. SIP over TLS repose sur le protocole TLS largement déployé et normalisé. SIP over TLS crypte uniquement les messages de signalisation et non pas le support. Un protocole de sécurité séparé tel que SRTP (Secure Real-Time Transport Protocol) peut être utilisé pour crypter les paquets vocaux. SIP sur TLS est configuré dans le paramètre SIP Transport, configuré dans les pages Line. Reportez-vous au **Pages Line (1-4), page 194.**

Enregistrement auprès du prestataire de services.

Pour utiliser un service de téléphonie sur Internet, vous devez enregistrer votre SRP auprès du fournisseur de services de téléphonie sur Internet (ITSP).

REMARQUE Chaque onglet de ligne doit être configuré séparément. Chaque onglet de ligne doit être configuré pour un fournisseur de services téléphoniques Internet différent.

ÉTAPE 1 Connectez-vous à l'utilitaire de configuration. Si vous y êtes invité, entrez l'identifiant de connexion administrateur fourni par le fournisseur d'accès. Le nom d'utilisateur et le mot de passe par défaut sont tous les deux **admin**.

ÉTAPE 2 Dans le menu Voice, sélectionnez l'interface **Line** que vous souhaitez modifier.

ÉTAPE 3 Dans la section Proxy and Registration, entrez le proxy.

ÉTAPE 4 Dans la section Subscriber Information, entrez l'ID utilisateur et le mot de passe.

Il s'agit des paramètres minimaux pour la plupart des connexions ITSP. Entrez les informations de compte conformément aux exigences de votre ITSP.

ÉTAPE 5 Cliquez sur **Submit** pour enregistrer les paramètres. Le service voix redémarre.

ÉTAPE 6 Pour vérifier votre progression, effectuez les tâches suivantes :

a. Dans le volet de navigation Voice, cliquez sur **Info**. Faites défiler l'écran vers le bas jusqu'à la section **Line** de la page pour la ligne que vous avez configurée. Vérifiez que cette ligne est enregistrée.

b. Utilisez un téléphone externe pour passer un appel entrant au numéro de téléphone attribué par votre fournisseur de services téléphoniques Internet. Si vous avez conservé les paramètres par défaut, le téléphone doit sonner et vous pouvez décrocher pour activer l'option audio bidirectionnelle.

c. Si la ligne n'est pas enregistrée, vous devrez peut-être actualiser le navigateur à plusieurs reprises, car quelques secondes peuvent s'avérer nécessaires avant l'exécution de l'enregistrement. Vérifiez également que le DNS est correctement configuré.

Gestion des services d'identification de l'appelant

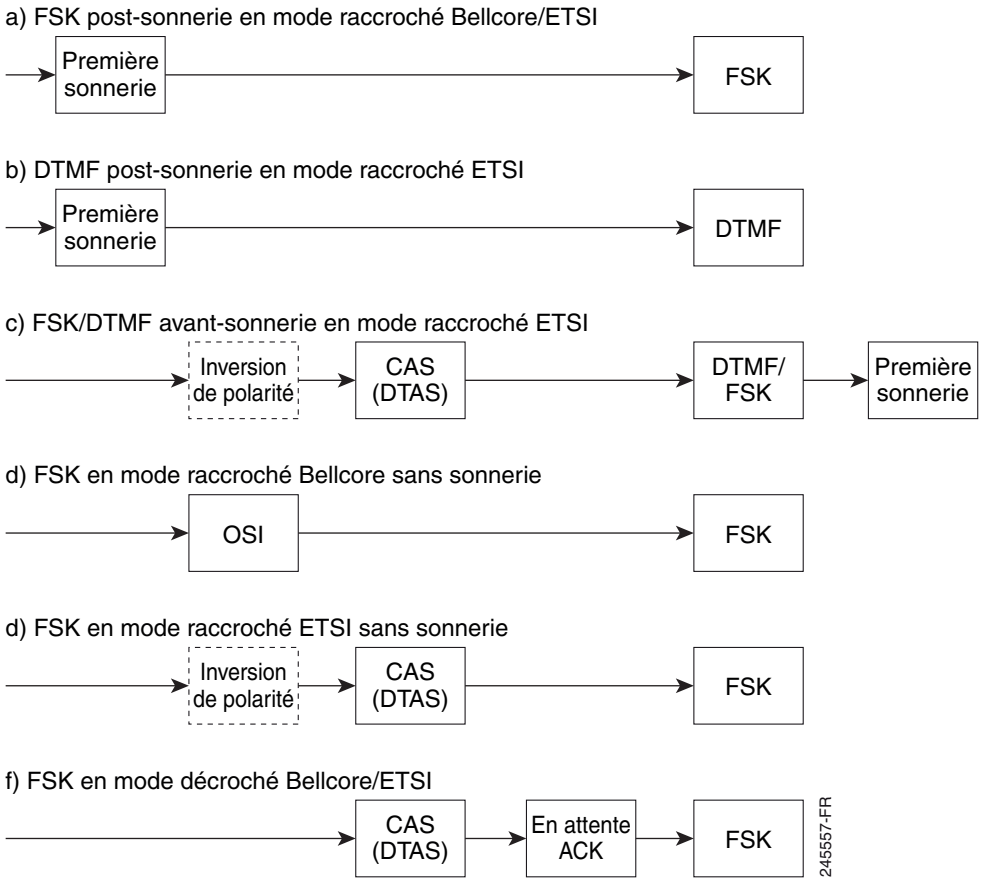
Le choix de la méthode d'identification de l'appelant (CID) dépend de votre région. Cette option est disponible à la page **Voice > Regional** de la zone Miscellaneous. Pour configurer le service CID, utilisez les paramètres ci-dessous :

Caller ID Method
Bellcore (North America, China) : CID, CIDCW et VMWI. FSK envoyé après la première sonnerie (identique à ETSI FSK envoyé après la première sonnerie) (sans inversion de la polarité ou DTAS). Il s'agit du paramètre par défaut.
DTMF (Finland, Sweden) : CID uniquement. DTMF envoyé après l'inversion de la polarité (sans DTAS) et avant la première sonnerie.
DTMF (Denmark) : CID uniquement. DTMF envoyé avant la première sonnerie sans inversion de polarité, ni DTAS.

Caller ID Method
ETSI DTMF : CID uniquement. DTMF envoyé après DTAS (sans inversion de la polarité) et avant la première sonnerie.
ETSI DTMF With PR : CID uniquement. DTMF envoyé après l'inversion de la polarité et DTAS et avant la première sonnerie.
ETSI DTMF After Ring : CID uniquement. DTMF envoyé après la première sonnerie (sans inversion de la polarité ou DTAS).
ETSI FSK : CID, CIDCW et VMWI. FSK envoyé après DTAS (sans inversion de la polarité) et avant la première sonnerie. En attente d'ACK de CPE après DTAS pour CIDCW.
ETSI FSK With PR (UK) : CID, CIDCW et VMWI. FSK est envoyé après l'inversion de la polarité et DTAS et avant la première sonnerie. En attente d'ACK de CPE après DTAS pour CIDCW. L'inversion de la polarité ne s'applique que si l'équipement est raccroché.
DTMF (Denmark) With PR : CID uniquement. DTMF envoyé après l'inversion de la polarité (sans DTAS) et avant la première sonnerie.
Caller ID FSK Standard
La SRP prend en charge les normes bell 202 et v.23 pour la génération de l'ID de l'appelant. Sélectionnez la norme FSK que vous souhaitez utiliser : bell 202 ou v.23. La valeur par défaut est bell 202.

Il existe trois types d'ID d'appelant :

- **ID de l'appelant associé à la sonnerie téléphone raccroché** : ce type d'ID de l'appelant est utilisé pour les appels entrants lorsque le téléphone connecté est raccroché. Reportez-vous aux figures (a) – (c) ci-dessous. Toutes les méthodes CID peuvent être utilisées avec ce type de CID.
- **ID de l'appelant non associé à la sonnerie téléphone raccroché** : utilisé pour envoyer un signal VMWI au téléphone afin d'allumer ou d'éteindre le voyant de message en attente (reportez-vous à la figure ci-dessous). Cette fonctionnalité est disponible uniquement pour les méthodes CID basées sur FSK : (Bellcore, ETSI FSK et ETSI FSK With PR).
- **ID de l'appelant téléphone décroché** : utilisé pour indiquer l'identité de l'appelant lorsque le téléphone connecté est décroché (reportez-vous à la figure ci-dessous). Cette fonctionnalité indique l'ID de l'appelant en attente (CIDCW) ou signale à l'utilisateur que l'identité de l'interlocuteur distant a changé ou a été mise à jour (par exemple, suite à un transfert d'appels). Cette fonctionnalité est disponible uniquement pour les méthodes CID basées sur FSK : (Bellcore, ETSI FSK et ETSI FSK With PR).


a) FSK post-sonnerie en mode raccroché Bellcore/ETSI
Première sonnerie
FSK
b) DTMF post-sonnerie en mode raccroché ETSI
Première sonnerie
DTMF
c) FSK/DTMF avant-sonnerie en mode raccroché ETSI
Inversion de polarité
CAS (DTAS)
DTMF/ FSK
Première sonnerie
d) FSK en mode raccroché Bellcore sans sonnerie
OSI
FSK
d) FSK en mode raccroché ETSI sans sonnerie
Inversion de polarité
CAS (DTAS)
FSK
f) FSK en mode décroché Bellcore/ETSI
CAS (DTAS)
En attente ACK
FSK
245557-FR

Optimisation des taux d'aboutissement des télécopies

Des problèmes peuvent survenir avec les transmissions de fax sur des réseaux IP, même avec la norme T.38, qui est prise en charge par la SRP. Vous pouvez régler plusieurs paramètres sur votre SRP pour optimiser vos taux d'aboutissement des télécopies.

ÉTAPE 1 Assurez-vous d'avoir suffisamment de bande passante pour les liaisons ascendante et descendante.

- Pour G.711 fallback, il est conseillé de disposer de 100 Kbits/s environ.
- T.38 nécessite au moins 50 Kbits/s.

ÉTAPE 2 Afin d'optimiser le taux d'aboutissement des télécopies de G.711 fallback, définissez les paramètres suivants dans l'onglet Line de votre SRP :

- **Network Jitter Buffer** : very high
- **Jitter buffer adjustment** : disable
- **Call Waiting** : no
- **3 Way Calling** : no
- **Echo Canceller** : no
- **Silence suppression** : no
- **Preferred Codec** : G.711
- **Use pref. codec only** : yes

REMARQUE Lorsque vous utilisez une passerelle multimédia Cisco pour les terminaisons PSTN, désactivez T.38 (relais fax) et activez le fax à l'aide du modem permettant le trafic via un port voix. Par exemple :

```
modem passthrough nse payload-type 110 codec g711ulaw
fax rate disable
fax protocol pass-through g711ulaw
```

ÉTAPE 3 Activez le fax T.38 sur la SRP en configurant les paramètres ci-dessous dans l'onglet Line du port FXS auquel le télécopieur est connecté :

```
FAX_Passthru_Method: ReINVITE
```

Lorsqu'il est impossible de configurer un appel T.38, l'appel doit être renvoyé automatiquement à G.711 fallback.

ÉTAPE 4 Lorsque vous utilisez une passerelle multimédia Cisco, utilisez les paramètres ci-dessous. Assurez-vous que la passerelle Cisco est correctement configurée pour T.38 avec le terminal de numérotation dial-peer SRP. Par exemple :

```
fax protocol T38
fax rate voice
fax-relay ecm disable
fax nsf 000000
no vad
```

Résolution des problèmes liés au fax

Si vous rencontrez des problèmes pour envoyer ou recevoir des télécopies, suivez les étapes ci-dessous :

ÉTAPE 1 Vérifiez que votre télécopieur est configuré sur un débit compris entre 7200 et 14400.

ÉTAPE 2 Envoyez un fax d'essai dans un environnement contrôlé entre deux SPR.

ÉTAPE 3 Déterminez le taux de réussite.

ÉTAPE 4 Surveillez le réseau et enregistrez les statistiques d'instabilité, de perte et de retard.

ÉTAPE 5 Si la télécopie échoue constamment, enregistrez une copie de la configuration de la SRP en téléchargeant le fichier suivant. Vous pouvez ensuite envoyer ce fichier à l'assistance technique.

```
http://<SRP_IP_Address>/admin/
config.xml&xuser=admin&xpassword=<admin_password>
```

Si vous utilisez un navigateur Web, choisissez l'option **view source** pour la page résultante et enregistrez ce fichier localement.

ÉTAPE 6 Activez et enregistrez la liste de débogage.

REMARQUE Vous pouvez également enregistrer les données à l'aide du tracé de l'analyseur réseau.

ÉTAPE 7 Identifiez le type de télécopieur connecté au périphérique.

ÉTAPE 8 Contactez l'assistance technique :

- Si vous êtes un utilisateur final de produits VoIP, contactez votre revendeur ou le prestataire de services téléphoniques Internet qui a fourni l'appareil.
- Si vous êtes un partenaire Cisco agréé, contactez l'assistance technique Cisco à l'adresse : www.cisco.com/support.

Configuration des plans de numérotation

Les plans de numérotation déterminent comment les chiffres composés sont interprétés et transmis. Ils déterminent également si le numéro composé est accepté ou rejeté. Vous pouvez utiliser un plan de numérotation pour faciliter la composition ou pour bloquer certains types d'appels comme les appels longue distance ou les appels internationaux. Cette section inclut des informations nécessaires à la compréhension des plans de numérotation, ainsi que des procédures de configuration de vos propres plans de numérotation.

Cette section comprend les rubriques suivantes :

- **À propos des plans de numérotation**
- **Modification des plans de numérotation**

À propos des plans de numérotation

Cette section fournit des informations pour vous aider à comprendre la mise en œuvre des plans
de numérotation. Reportez-vous aux rubriques suivantes :

- **Séquences de chiffres**
- **Exemples de séquence de chiffres**
- **Réception et transmission des chiffres composés**
- **Temporisateur du plan de numérotation (temporisateur de décrochage)**
- **Temporisateur long inter-chiffres (temporisateur de saisie incomplète)**
- **Temporisateur court inter-chiffres (temporisateur de saisie complète)**

Séquences de chiffres

Un plan de numérotation contient une série de séquences de chiffres, séparées par un guillemet. La totalité des séquences est entourée par des parenthèses. Chaque séquence de chiffres du plan de numérotation inclut une série d'éléments, qui correspondent individuellement aux touches sur lesquelles l'utilisateur appuie.

REMARQUE Les espaces vides sont ignorés, mais peuvent être utilisés pour améliorer la lisibilité.

Séquence de chiffres	Fonction
0 1 2 3 4 5 6 7 8 9 0 * #	Saisissez n'importe lequel de ces caractères pour représenter une touche devant être utilisée sur le clavier du téléphone.
x	Entrez `x` pour représenter n'importe quel caractère du clavier du téléphone.
[séquence]	Saisissez des caractères à l'intérieur des crochets pour créer une liste de touches utilisées acceptées. L'utilisateur peut appuyer sur n'importe quelle touche de cette liste. Plage numérique : par exemple, vous devez entrer `[2-9]` pour autoriser l'utilisation de tout chiffre compris entre 2 et 9. Plage numérique avec d'autres caractères : Par exemple, vous devez entrer `[35-8*]` pour autoriser l'utilisation des chiffres 3, 5, 6, 7, 8, ou *.
. (point)	Saisissez un point pour la répétition d'un élément. Le plan de numérotation autorise l'entrée d'un ou plusieurs zéros. Par exemple, `01.` permet aux utilisateurs d'entrer 0, 01, 011, 0111 et ainsi de suite.

Séquence de chiffres	Fonction
<<dialed:substituted>>	Utilisez ce format pour indiquer que certains chiffres composés sont remplacés par d'autres caractères lors de la transmission de la séquence. Les chiffres composés peuvent être le zéro ou d'autres caractères. **EXEMPLE 1** : `<8:1650>xxxxxxx` Lorsque l'utilisateur appuie sur le 8, suivi d'un numéro à sept chiffres, le système remplace automatiquement le 8 par 1650. Si l'utilisateur compose le **85550112**, le système transmet **16505550112**. **EXEMPLE 2** : `<:1>xxxxxxxxxx` Dans cet exemple, aucun chiffre n'est remplacé. Lorsque l'utilisateur compose un numéro à dix chiffres, le numéro 1 est ajouté au début de la séquence. Si l'utilisateur compose le **9725550112**, le système transmet le **19725550112**.
, (virgule)	Entrez une virgule entre les chiffres pour émettre une tonalité de « ligne extérieure » après la saisie de la séquence par l'utilisateur. **EXEMPLE :** `9, 1xxxxxxxxx` Lorsque l'utilisateur appuie sur la touche 9, une tonalité de numérotation de « ligne extérieure » est émise jusqu'à ce qu'il appuie sur la touche 1.
! (point d'exclamation)	Entrez un point d'exclamation pour interdire un modèle de séquence de numérotation. **EXEMPLE :** `1900xxxxxxx!` Le système rejette toute séquence à onze chiffres commençant par 1900.
*xx	Saisissez un astérisque pour permettre à l'utilisateur de saisir un code étoile à deux chiffres.
S0 ou L0	Entrez S0 pour réduire le minuteur inter-chiffres court à 0 secondes ou entrez L0 pour réduire le minuteur inter-chiffres long à 0 secondes.

Exemples de séquence de chiffres

Les exemples suivants illustrent des séquences de chiffres que vous pouvez saisir dans votre plan de numérotation.

Dans la saisie complète d'un plan de numérotation, les séquences sont séparées par le caractère tube (|), et l'ensemble des séquences est fermé par des parenthèses.

EXEMPLE: `([1-8]xx | 9, xxxxxxx | 9, <:1>[2-9]xxxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9] xxxxxxxxx | 9, 1 900 xxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11 )`

Postes de votre système

```
EXEMPLE : ( [1-8]xx | 9, xxxxxxx | 9, <:1>[2-9]xxxxxxxxx | 8,
<:1212>xxxxxxx | 9, 1 [2-9] xxxxxxxxx | 9, 1 900 xxxxxxx ! | 9,
011xxxxxx. | 0 | [49]11 )
```

`[1-8]xx` Permet à un utilisateur de composer tout nombre à trois chiffres qui commence par un chiffre compris entre 1 et 8. Si votre système utilise des extensions à quatre chiffres, vous devez entrer la chaîne suivante à la place : **[1-8]xxx**

Numérotation locale d'un numéro à sept chiffres

```
EXAMPLE: ( [1-8]xx | 9, xxxxxxx | 9, <:1>[2-9]xxxxxxxxx | 8, <:1212>xxxxxxx |
9, 1 [2-9] xxxxxxxxx | 9, 1 900 xxxxxxx ! | 9, 011xxxxxx. | 0 | [49]111)
```

`9, xxxxxxx` Lorsqu'un utilisateur appuie sur la touche 9, une tonalité externe est émise. L'utilisateur peut alors composer un nombre à sept chiffres, comme dans le cas d'un appel local.

Numérotation locale avec un indicatif régional à trois chiffres et un numéro local à sept chiffres.

EXAMPLE: `( [1-8]xx | 9, xxxxxxx | 9, <:1>[2-9]xxxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9] xxxxxxxxx | 9, 1 900 xxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11 )`

`9, <:1>[2-9]xxxxxxxxx` Cet exemple est utile lorsque l'utilisation d'un indicatif local est obligatoire. Lorsqu'un utilisateur appuie sur la touche 9, une tonalité de numérotation externe est émise. L'utilisateur doit entrer un numéro à 10 chiffres qui commence par un chiffre compris entre 2 et 9. Le système insère automatiquement le préfixe 1 avant de transmettre le numéro à l'opérateur.

Numérotation locale avec l'insertion automatique d'un indicatif régional à trois chiffres.

EXAMPLE: `( [1-8]xx | 9, xxxxxxx | 9, <:1>[2-9]xxxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9] xxxxxxxxx | 9, 1 900 xxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11 )`

`8, <:1212>xxxxxxx` Cet exemple est utile lorsque l'opérateur exige un indicatif régional, alors que la majorité des appels est dirigé vers une seule région. Lorsqu'un utilisateur appuie sur la touche 8, une tonalité de numérotation extérieure est émise. L'utilisateur peut saisir n'importe quel numéro à sept chiffres. Le système insert automatiquement le préfixe 1 et l'indicatif local 212 avant de transmettre le numéro à l'opérateur.

Numérotation longue distance aux États-Unis

EXAMPLE: `( [1-8]xx | 9, xxxxxxx | 9, <:1>[2-9]xxxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9] xxxxxxxxx | 9, 1 900 xxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11 )`

`9, 1 [2-9] xxxxxxxxx` Lorsque l'utilisateur appuie sur la touche 9, une tonalité externe est émise. L'utilisateur peut saisir n'importe quel numéro à onze chiffres commençant par 1, suivi d'un chiffre de 2 à 9.

Numéro bloqué

EXAMPLE: `( [1-8]xx | 9, xxxxxxx | 9, <:1>[2-9]xxxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9] xxxxxxxxx | 9, 1 900 xxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11 )`

`9, 1 900 xxxxxxx !` Cette séquence de chiffres est utile si vous souhaitez empêcher les utilisateurs de composer des numéros surtaxés ou au contenu inapproprié (par exemple, les numéros 1-900 aux États-Unis). Lorsque l'utilisateur appuie sur la touche 9, une tonalité externe est émise. Si l'utilisateur saisit un numéro à onze chiffres commençant par 1900, l'appel est rejeté.

Appels internationaux aux États-Unis

EXAMPLE: `( [1-8]xx | 9, xxxxxxx | 9, <:1>[2-9]xxxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9] xxxxxxxxx | 9, 1 900 xxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11 )`

`9, 011xxxxxx.` Lorsqu'un utilisateur appuie sur la touche 9, une tonalité de numérotation extérieure est émise. L'utilisateur peut saisir n'importe quel numéro commençant par 011, comme pour un appel international depuis les États-Unis.

Numéros informationnels

EXAMPLE: `( [1-8]xx | 9, xxxxxxx | 9, <:1>[2-9]xxxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9] xxxxxxxxx | 9, 1 900 xxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11 )`

`0 | [49]11` Cet exemple inclut deux séquences de chiffres, séparées par le caractère tube. La première séquence permet à l'utilisateur de composer le 0 pour un opérateur. La seconde permet à l'utilisateur de saisir le 441 pour les informations locales ou le 911 pour les services d'urgence.

Réception et transmission des chiffres composés

Lorsqu'un utilisateur compose une série de chiffres, le système recherche une séquence identique parmi l'ensemble des séquences du plan de numérotation. Les séquences identiques forment un ensemble de séquences numériques candidates. Plus l'utilisateur saisit de chiffres, plus le nombre de séquences candidates diminue jusqu'à ce qu'une seule ou aucune séquence ne soit valide. Lorsqu'un événement d'interruption se produit, le SRP accepte la séquence composée par l'utilisateur et démarre l'appel, ou bien il rejette la séquence comme étant non valide. La tonalité de réorganisation (ligne occupée rapide) est émise si la séquence composée est non valide.

Le tableau suivant explique comment les événements d'arrêt sont traités.

Événements d'arrêt	Traitement
Les chiffres composés ne correspondent à aucune séquence du plan de numérotation.	Le numéro est rejeté.
Les chiffres composés correspondent à une seule séquence du plan de numérotation.	Si la séquence est autorisée par le plan de numérotation, le numéro est accepté et transmis en fonction du plan. Si la séquence est bloquée par le plan de numérotation, le numéro est rejeté.

Événements d'arrêt	Traitement
Un dépassement du délai imparti se produit.	Le numéro est rejeté s'il ne correspond à aucune séquence du plan de numérotation pendant le temps imparti par le temporisateur inter-chiffres applicable. Le minuteur long inter-chiffres intervient lorsque les chiffres composés ne correspondent à aucune séquence du plan de numérotation. La valeur par défaut est 10 secondes. Le temporisateur court inter-chiffres intervient lorsque les chiffres composés correspondent à une ou plusieurs séquences candidates du plan de numérotation. La valeur par défaut est de 3 secondes.
L'utilisateur appuie sur la touche #.	Si la séquence complète est autorisée par le plan de numérotation, le numéro est accepté et transmis en fonction du plan. Si la séquence est incomplète ou bloquée par le plan de numérotation, le numéro est rejeté.

Temporisateur du plan de numérotation (temporisateur de décrochage)

Le temporisateur du plan de numérotation est un « temporisateur de décrochage ». Il débute lorsque le combiné est décroché. Si aucun chiffre n'est composé pendant le nombre de secondes spécifié, le temporisateur expire et l'absence d'entrée est évaluée. L'appel est rejeté, sauf si vous possédez une chaîne du plan de numérotation spéciale qui autorise l'absence d'entrée. La valeur par défaut est 5.

Syntaxe du temporisateur du plan de numérotation

SYNTAXE : `(Ps<:n> | dial plan )`

- s : nombre de secondes ; si aucun nombre n'est saisi après `P`, le minuteur par défaut de 5 secondes s'applique.
- n : (facultatif) : numéro à transmettre automatiquement lorsque le minuteur expire ; vous pouvez entrer un numéro valide. Aucun caractère de remplacement n'est autorisé car le numéro est transmis tel quel. Si vous omettez la substitution du numéro, <:n>, la tonalité de réorganisation (ligne occupée rapide) est émise après le nombre de secondes spécifié.

Exemples de temporisateur du plan de numérotation

- **Donnez plus de temps à l'utilisateur pour commencer la numérotation après avoir décroché le combiné.**

  EXEMPLE : `(P9 | (9,8<:1408>[2-9]xxxxxx | 9,8,1[2 9]xxxxxxxxx | 9,8,011xx. | 9,8,xx.|[1-8]xx)`

  `P9` Après avoir décroché le combiné, l'utilisateur dispose de 9 secondes pour commencer la numérotation. Si aucun chiffre n'est actionné pendant ces 9 secondes, l'utilisateur entend une tonalité de réorganisation (ligne occupée rapide). En paramétrant un temporisateur plus long, vous donnez plus de temps à l'utilisateur pour la numérotation.

- **Créer un service téléphonique pour toutes les séquences du plan de numérotation du système.**

  EXEMPLE : `(P9<:23> | (9,8<:1408>[2-9]xxxxxx | 9,8,1[2-9]xxxxxxxxx | 9,8,011xx. | 9,8,xx.|[1-8]xx)`

  `P9<:23>` Après avoir décroché le combiné, l'utilisateur dispose de 9 secondes pour commencer la numérotation. Si aucun chiffre n'est sélectionné pendant ces 9 secondes, l'appel est transmis automatiquement au poste 23.

- **Créer un service téléphonique sur un bouton Ligne pour le poste.**

  EXEMPLE : `(P0 <:1000>)`

  Lorsque le temporisateur est réglé sur 0 seconde, l'appel est transmis automatiquement au poste spécifié dès que le combiné est décroché. Saisissez cette séquence dans le plan de numérotation du téléphone pour le poste 2 d'une station de client.

Temporisateur long inter-chiffres (temporisateur de saisie incomplète)

Ce temporisateur correspond à celui « de saisie incomplète ». Il mesure l'intervalle entre les numéros composés. Il s'applique tant que les chiffres composés ne correspondent à aucune séquence du plan de numérotation. La saisie est jugée incomplète et l'appel est rejeté, sauf si l'utilisateur saisit un autre chiffre dans le temps imparti. La valeur par défaut est 10 secondes.

REMARQUE Cette section explique comment modifier un temporisateur dans le cadre du plan de numérotation. Vous pouvez également modifier le temporisateur de contrôle qui vérifie les temporisateurs inter-chiffres par défaut pour tous les appels. Voir aussi **Réinitialisation des temporisateurs de contrôle, page 147**.

Syntaxe du temporisateur long inter-chiffres

SYNTAX: L:s, (*dial plan*)

s : nombre de secondes ; si aucun nombre n'est saisi après `L:`, le minuteur par défaut de 5 secondes s'applique. La séquence du minuteur apparaît à gauche de la première parenthèse du plan de numérotation.

Exemple de temporisateur long inter-chiffres

EXAMPLE: `L:15, (9,8<:1408>[2-9]xxxxxx | 9,8,1[2-9]xxxxxxxxx | 9,8,011xx. | 9,8,xx.|[1-8]xx)`

`L:15,` Ce plan de numérotation permet à l'utilisateur de faire une pause allant jusqu'à 15 secondes entre chaque chiffre avant l'expiration du temporisateur long inter-chiffres.

Temporisateur court inter-chiffres (temporisateur de saisie complète)

Ce temporisateur correspond à celui « de saisie complète ». Il mesure l'intervalle entre les numéros composés. Il s'applique lorsque les chiffres composés correspondent à au moins une séquence du plan de numérotation. La saisie est évaluée, sauf si l'utilisateur saisit un autre chiffre dans le temps imparti. Si elle est valide, l'appel est effectué. Si elle est non valide, l'appel est rejeté. La valeur par défaut est de 3 secondes.

Syntaxe du temporisateur court inter-chiffres

SYNTAX 1: `S:s,` (*dial plan*)

Utilisez cette syntaxe pour appliquer les nouveaux paramètres au plan de numérotation entier figurant dans les parenthèses.

SYNTAX 2: sequence `Ss`

Utilisez cette syntaxe pour appliquer les nouveaux paramètres à une séquence de numérotation particulière.

s : nombre de secondes ; si aucun nombre n'est entré après `S`, le minuteur par défaut de 5 secondes s'applique.

Exemples de temporisateurs court inter-chiffres

- Configurez le temporisateur pour le plan de numérotation entier.

  EXAMPLE: `S:6,(9,8<:1408>[2-9]xxxxxx | 9,8,1[2-9]xxxxxxxxx | 9,8,011xx. | 9,8,xx.|[1-8]xx)`

  `S:6,` Pendant la numérotation avec le combiné décroché, l'utilisateur peut effectuer une pause allant jusqu'à 15 secondes entre chaque chiffre avant l'expiration du minuteur court inter-chiffres.

- Configurez un temporisateur instantané pour une séquence particulière du plan de numérotation.

  EXAMPLE: `(9,8<:1408>[2-9]xxxxxx | 9,8,1[2-9]xxxxxxxxxS0 | 9,8,011xx. | 9,8,xx.|[1-8]xx)`

  `9,8,1[2-9]xxxxxxxxxS0` Lorsque le minuteur est réglé sur 0, l'appel est transmis automatiquement au moment où l'utilisateur compose le dernier chiffre de la séquence.

Modification des plans de numérotation

Vous pouvez modifier les plans de numérotation et les temporisateurs de contrôle.

Saisie du plan de numérotation de l'interface de ligne

Ce plan de numérotation est utilisé pour retirer les chiffres de redirection d'un numéro composé avant qu'il ne soit transmis à la porteuse.

ÉTAPE 1 Connectez-vous à l'utilitaire de configuration. Si vous y êtes invité, entrez l'identifiant de connexion administrateur fourni par le fournisseur d'accès. Le nom d'utilisateur et le mot de passe par défaut sont tous les deux **admin**.

ÉTAPE 2 Dans le menu Voice, sélectionnez l'interface Line que vous souhaitez modifier.

ÉTAPE 3 Faites défiler jusqu'à la section Dial Plan.

ÉTAPE 4 Entrez les séquences de chiffres dans le champ **Dial Plan**. Pour obtenir plus d'informations, reportez-vous à la section **À propos des plans de numérotation, page 137.**

ÉTAPE 5 Cliquez sur **Submit** pour enregistrer les paramètres.

Réinitialisation des temporisateurs de contrôle

Utilisez la procédure suivante pour réinitialiser les paramètres par défaut du temporisateur, pour tous les appels.

REMARQUE Pour modifier un paramètre du minuteur pour une séquence de chiffres ou un type d'appel spécifique uniquement, vous pouvez modifier le plan de numérotation. Voir aussi **À propos des plans de numérotation, page 137**.

ÉTAPE 1 Connectez-vous à l'utilitaire de configuration. Si vous y êtes invité, entrez l'identifiant de connexion administrateur fourni par le fournisseur d'accès. Le nom d'utilisateur et le mot de passe par défaut sont tous les deux **admin**.

ÉTAPE 2 Dans le menu Voice, cliquez sur **Regional**.

ÉTAPE 3 Faites défiler jusqu'à la section Control Timer Values.

ÉTAPE 4 Entrez les valeurs souhaitées dans les champs Interdigit Long Timer et Interdigit Short Timer. Référez-vous aux définitions au début de cette section.

Implémentation d'appel sécurisé

Cette section décrit la mise en œuvre d'un appel sécurisé avec la SRP. Il comprend les sections suivantes :

- **Activation des appels sécurisés**
- **Détails des appels sécurisés**
- **Utilisation d'un Mini-certificat**
- **Génération d'un mini certificat**

REMARQUE Il s'agit d'une rubrique avancée, conçue uniquement pour les installateurs expérimentés.

Activation des appels sécurisés

Un appel sécurisé est établi en deux étapes. La première étape n'est pas différente de la configuration d'un appel normal. La seconde étape commence après avoir établi l'appel de manière normale. Chaque côté de l'appel doit être prêt à diffuser les paquets RTP.

Au cours de la seconde étape, les deux participants échangent des informations pour déterminer si l'appel en cours peut basculer en mode sécurisé. Ces informations sont transportées par encodage base64 intégré au corps de la requête SIP INFO. Les réponses à ce message utilisent un format propriétaire. Si cette seconde étape est réussie, la SRP émet une tonalité d'indication d'appel sécurisé pendant un court instant, afin d'indiquer aux deux participants que l'appel est sécurisé et que le trafic RTP est crypté dans les deux directions.

Si l'utilisateur possède un téléphone qui prend en charge le CIDCW (Identifiant de l'appelant de l'appel en attente) et que ce service est activé, alors l'ID de l'appelant peut être mis à jour par les informations extraites du Mini-Certificat reçu par l'interlocuteur. Le champ du nom de l'identifiant de l'appelant (CID) commencera par le symbole « $ ». Chacun des participants peut vérifier le nom et le numéro pour s'assurer de l'identité de son interlocuteur.

L'agent de signature est implicite et doit être identique pour tous les périphériques qui communiquent entre eux de manière sécurisée. La clé publique de l'agent de signature est préconfigurée dans la SRP par l'administrateur et elle est utilisée par la SRP pour vérifier le Mini-certificat de son homologue. Le Mini-certificat est valide s'il n'a pas expiré et s'il possède une signature valide.

La SRP peut être configurée de sorte que, par défaut, tous les appels sortants soient sécurisés ou non. Si par défaut ils sont sécurisés, l'utilisateur peut désactiver la sécurité lors d'un appel en composant *19 avant le numéro cible. Si par défaut ils ne sont pas sécurisés, l'utilisateur peut passer un appel sortant sécurisé en composant *18 avant le numéro cible. Cependant, l'utilisateur ne peut pas décider si un appel entrant sera sécurisé ou non ; c'est l'appelant qui active ou non la sécurité.

La SRP ne bascule pas en mode sécurisé si le Mini-certificat du CID de l'appelé ne correspond pas à l'ID utilisateur de l'appel extérieur. La SRP effectue cette vérification après avoir reçu le Mini-certificat de l'appelé.

Détails des appels sécurisés

Cette étape peut être divisée en deux parties car elle explique la seconde étape de paramétrage d'un appel sécurisé avec plus de détails.

ÉTAPE 1 L'appelant envoie un message « Caller Hello » (code base64 intégré au corps d'une requête SIP INFO) à l'appelé contenant les informations suivantes :

- Identifiant du message (4B)
- Version et indicateurs (4B)
- SSRC du flux crypté (4B)
- Mini-certificat (252B)

Dès la réception du message « Caller Hello», l'appelé répond par un message « Callee Hello » (code base64 intégré au corps de la réponse SIP à la requête INFO de l'appelant) contenant les informations similaires si le message « Caller Hello» est valide. L'appelant examine alors le message « Callee Hello » et passe à l'étape suivante si le message est valide.

ÉTAPE 2 L'appelant envoie le message « Caller Final » à l'appelé avec les informations suivantes :

- Identifiant du message (4B)
- Clé cryptée principale (16B ou 128b)
- Sel crypté principal (16B ou 128b)

Utilisation d'un Mini-certificat

La clé et le sel principaux sont cryptés avec une clé publique provenant du Mini-certificat de l'appelé. La clé et le sel principaux sont utilisés par chacune des extrémités pour dériver les clés de session en vue du cryptage des paquets RTP suivants. L'appelé répond alors avec un message « Callee Final » (qui est un message vide).

Le Mini-certificat (MC) contient les informations suivantes :

- Nom d'utilisateur (32B)
- Identifiant de l'utilisateur ou numéro de téléphone (16B)
- Date d'expiration (12B)
- Clé publique (512b ou 64B)
- Signature (1024b ou 512B)

Le MC possède une clé publique 512 bits pour établir les appels sécurisés. L'administrateur doit mettre en service chaque abonné du service d'appel sécurisé avec le MC et la clé privée 512 bits correspondante. Le MC est validé avec une clé privée de 1024 bits du fournisseur d'accès, qui agit comme l'autorité de certification (CA) du MC. La clé publique 1024 bits de la signature du CA sur le MC doit également être mise en service pour chaque abonné.

La clé publique du CA est utilisée pour vérifier le MC reçu depuis l'autre extrémité. Si le MC est non valide, l'appel ne va pas basculer en mode sécurisé. Le MC et la clé publique CA 1024 bits sont concaténés et codés base64 dans l'unique paramètre Mini Certificate. La clé privée 512 bits est codée base64 dans le paramètre SRTP Private Key, qui doit être gardé secret, comme un mot de passe. (Les paramètres Mini Certificate et SRTP Private Key sont configurés dans les pages Line (1-4).)

L'établissement d'un appel sécurisé s'appuyant sur l'échange d'informations insérées dans le corps des messages de requêtes/réponses SIP INFO, le prestataire de service doit s'assurer que l'infrastructure du réseau permet l'acheminement des messages SIP INFO sans modification de leurs corps.

Génération d'un mini certificat

Cisco fournit un Générateur de mini-certificat pour générer les mini-certificats et les clés privées. Contactez votre représentant Cisco pour accéder à cet outil.

Le Générateur de mini-certificat utilise la syntaxe suivante :

`gen_mc` *`ca-key user-name user-id expire-date`*

Où :

- ca-key est un fichier texte comportant les paires de clés privée/publique CA 1024 bits codées base64 pour signer/vérifier le MC, par exemple :

```
9CC9aYU1X5lJuU+EBZmi3AmcqE9U1LxEOGwopaGyGOh3VyhKgi6JaVtQZt87PiJINKW8XQj3B9Qq
e3VgYxWCQNa335YCnDsenASeBxuMIEaBCYd1l1fVEodJZOGwXwfAde0MhcbD0kj7LVlzcsTyk2TZ
YTccnZ75TuTjj13qvYs=5nEtOrkCa84/mEwl3D9tSvVLyliwQ+u/
Hd+C8u5SNk7hsAUZaA9TqH8Iw0J/
IqSrsf6scsmundY5j7Z5mK5J9uBxSB8t8vamFGD0pF4zhNtbrVvIXKI9kmp4vph1C5jzO9gDfs3M
F+zjyYrVUFdM+pXtDBxmM+fGUfrpAuXb7/k=
```

- user-name est le nom de l'abonné, par exemple « Joe Smith ». Celle-ci peut contenir au maximum 32 caractères.
- user-id est l'identifiant d'utilisateur de l'abonné, qui doit correspondre à l'ID utilisateur du message INVITE lors de l'appel, par exemple « 14083331234 ». La longueur maximale est de 16 caractères.
- expire-date est la date d'expiration du MC, par exemple « 00:00:00 1/1/34 » 34=2034). En interne, la date est codée comme une chaîne 12B fixe : 000000010134

L'outil génère les paramètres Mini Certificate et SRTP Private Key qui peuvent être mis en service.

Exemple :

```
gen_mc ca_key “Joe Smith” 14085551234 “00:00:00 1/1/34”
```

Cet exemple engendre la clé privée SRTP et le Mini-certificat suivants :

```
<Mini Certificate>
Sm9lIFNtaXRoAAAAAAAAAAAAAAAAAAAAAAAAAAAAAxNDA4NTU1MTIzNAAAAAAAMDAwMDAwMDEw
MTM00OvJakde2vVMF3Rw4pPXL7lAgIagMpbLSAG2+++YlSqt198Cp9rP/
xMGFfoPmDKGx6JFtkQ5sxLcuwgxpxpxkeXvpZKlYlpsb28L4Rhg5qZA+Gqj1hDFCmG6dffZ9SJhx
ES767G0JIS+N8lQBLr0AuemotknSjjjOy8c+1lTCd2t44Mh0vmwNg4fDck2YdmTMBR516xJt4/
uQ/
LJQlni2kwqlm7scDvll5k232EvvvVtCK0AYa4eWd6fQOpiESCO9CC9aYU1X5lJuU+EBZmi3AmcqE
9U1LxEOGwopaGyGOh3VyhKgi6JaVtQZt87PiJINKW8XQj3B9Qqe3VgYxWCQNa335YCnDsenASeBx
uMIEaBCYd1l1fVEodJZOGwXwfAde0MhcbD0kj7LVlzcsTyk2TZYTccnZ75TuTjj13qvYs=
<SRTP Private Key>
b/DWc96X4YQraCnYzl5en1CIUhVQQqrvcr6Qd/8R52IEvJjOw/
e+Klm4XiiFEPaKmU8UbooxKG36SEdKusp0AQ==
```

Configuration des paramètres de voix

Utilisez les pages Voice pour afficher et configurer les paramètres de voix pour votre SRP. Ces pages sont décrites dans les sections suivantes :

- **Page Info**
- **Page System**
- **Page SIP**
- **Page Provisioning**
- **Page Regional**
- **Pages Line (1-4)**
- **Page PSTN (modèles SRP540 uniquement)**
- **Pages User**

REMARQUE Pour accéder aux pages des paramètres de voix, cliquez sur Voice dans l'onglet, puis cliquez sur la page à laquelle vous souhaitez accéder dans le volet de navigation.

Page Info

Utilisez la page Info pour afficher les informations relatives à l'application vocale SRP. Cette page comprend les sections suivantes :

- **Informations produit**
- **État du système**
- **État de la ligne**

Informations produit

Voice > Info > Product Information

Product Name	Numéro/nom de modèle.
Software Version	Numéro de version logicielle.
Voice Module Version	Numéro de version du module voix.
Client Certificate	État du certificat client, qui peut indiquer si la SRP est autorisée par votre fournisseur de services téléphoniques Internet.
Serial Number	Numéro de série du produit.
Hardware Version	Numéro de version matérielle.
MAC Address	Adresse MAC. Par exemple : 8843E1657936.
Customization	Fonctionnalité non utilisée.

État du système

Voice > Info > System Status

Current Time	Date et heure actuelles du système. Par exemple : 03/10/2003 16:43:00. Définissez l'heure système à l'aide de la page **Administration > Time Setup**.
RTP Packets Sent	Nombre total de paquets RTP envoyés (y compris les paquets redondants).
RTP Packets Recv	Nombre total de paquets RTP reçus (y compris les paquets redondants).
SIP Messages Sent	Nombre total de messages SIP envoyés (y compris les retransmissions).

SIP Messages Recv	Nombre total de messages SIP reçus (y compris les retransmissions).
External IP	Adresse IP externe utilisée pour le mappage NAT.
Elapsed Time	Temps écoulé total depuis le dernier redémarrage du système. Par exemple : 25 jours et 18:12:36.
RTP Bytes Sent	Nombre total d'octets RTP envoyés.
RTP Bytes Recv	Nombre total d'octets RTP reçus.
SIP Bytes Sent	Nombre total d'octets de messages SIP envoyés (y compris les retransmissions).
SIP Bytes Recv	Nombre total d'octets de messages SIP reçus (y compris les retransmissions).

État de la ligne

Voice > Info > Line 1 Status (des informations similaires ont également été fournies pour les lignes 2, 3 et 4)

Hook State	État du crochet du port FXO. Les lignes sont activées ou désactivées.
Last Registration At	Date et heure du dernier enregistrement de la ligne.
Message Waiting	Les états sont Yes ou No. La valeur est automatiquement définie sur Yes lorsqu'un message est reçu. Vous pouvez également effacer ou définir l'indicateur manuellement dans le menu utilisateur.
Last Called Number	Dernier numéro appelé depuis la ligne FXO.
Registration State	Indique si la ligne est enregistrée avec le proxy SIP.
Next Registration In	Nombre de secondes avant le prochain enregistrement. Indique si un nouveau message vocal est en attente.
Call Back Active	Indique si une demande de rappel est en cours. Les options sont Yes ou No.
Last Caller Number	Numéro du dernier appelant.
Mapped SIP Port	Numéro du port SIP mappé par NAT.

Call 1 and 2 State	Peut prendre l'une des valeurs suivantes : ▪ Idle ▪ Collecting PSTN Pin ▪ Invalid PSTN PIN ▪ PSTN Caller Accepted ▪ Connected to PSTN
Call 1 and 2 Tone	Type de tonalité utilisée par l'appel.
Call 1 and 2 Encoder	Codec utilisé pour l'encodage.
Call 1 and 2 Decoder	Codec utilisé pour le décodage.
Call 1 and 2 FAX	État du mode Fax Pass-Through.
Call 1 and 2 Type	Direction de l'appel. Peut prendre l'une des valeurs suivantes : ▪ PSTN Gateway Call = VoIP-To-PSTN Call ▪ VoIP Gateway Call = PSTN-To-VoIP Call ▪ PSTN To Line 1 = PSTN call ring through and answered by Line 1 ▪ Line 1 Forward to PSTN Gateway = VoIP calls Line 1 then forwarded to PSTN GW ▪ Line 1 Forward to PSTN Number =VoIP calls Line 1 then forwarded to PSTN number ▪ Line 1 To PSTN Gateway ▪ Line 1 To PSTN Gateway
Call 1 and 2 Remote Hold	Indique si le poste distant a placé l'appel en attente.
Call 1 and 2 Callback	Indique si l'appel a été déclenché par une demande de rappel.
Call 1 and 2 Peer Name	Nom du téléphone de l'homologue.
Call 1 and 2 Peer Phone	Numéro de téléphone du téléphone de l'homologue.
Call 1 and 2 Call Duration	Durée de l'appel
Call 1 and 2 Packets Sent	Nombre de paquets envoyés.

Call 1 and 2 Packets Recv	Nombre de paquets reçus.
Call 1 and 2 Bytes Sent	Nombre d'octets envoyés.
Call 1 and 2 Bytes Recv	Nombre d'octets reçus.
Call 1 and 2 Decode Latency	Nombre de millisecondes de latence du décodeur.
Call 1 and 2 Jitter	Nombre de millisecondes d'instabilité du récepteur.
Call 1 and 2 Round Trip Delay	Nombre de millisecondes de délai.
Call 1 and 2 Packets Lost	Nombre de paquets perdus
Call 1 and 2 Packet Error	Nombre de paquets reçus non valides.
Call 1 and 2 Mapped RTP Port	Port mappé pour le trafic RTP (Real Time Protocol) de l'appel 1/2.
Call 1 and 2 Media Loopback	Une boucle multimédia est utilisée pour la mesure quantitative et qualitative de la qualité vocale de l'utilisateur final.

État de la ligne PSTN (SRP540 uniquement)

(PSTN) Hook State	État du crochet du port FXO. Les valeurs sont soit On, soit Off.
(PSTN) Line Voltage	Tension électrique existante dans la ligne PSTN.
(PSTN) Loop Current	Courant (milliampères) existant dans la boucle locale.

Page System

Utilisez la page System pour configurer les paramètres de votre système et de votre réseau. Cette page comprend les sections suivantes :

- **Section Divers**
- **Section Miscellaneous**

Section Divers

Voice > System > System Configuration

Restricted Access Domains	Fonctionnalité actuellement inutilisée par la SRP.
IVR Admin Password	Mot de passe pour que l'administrateur gère la SRP à l'aide de l'IVR intégré via un combiné connecté. La valeur par défaut est **1234**.
IVR User Password	Mot de passe pour que l'utilisateur du téléphone gère sa ligne à l'aide de l'IVR intégré via son combiné. La valeur par défaut est **no password**.

Section Miscellaneous

Voice > System > Miscellaneous Settings

Syslog Server	Entrez l'adresse IP du serveur syslog, auquel les messages système seront envoyés.
Debug Server	Entrez l'adresse IP du serveur syslog, auquel les messages système seront envoyés.
Debug Level	Détermine le niveau des informations de débogage qui seront générées. Sélectionnez 0 1, 2, 3ou 3+Router dans la liste déroulante. Plus le niveau de débogage est élevé, plus le volume d'informations de débogage générées est important. La valeur par défaut est 0, ce qui signifie qu'aucune information de débogage n'est générée. Les niveaux 1, 2 et 3 génèrent des messages uniquement relatifs aux ports voix. 3+Router génère le contenu de débogage pour les composants voix et du routeur. Pour configurer les options de consignation, reportez-vous aux pages **Administration > Log**.

Page SIP

Utilisez la page SIP pour configurer de nombreux paramètres et valeurs SIP. Cette page comprend les sections suivantes :

- Paramètres SIP
- Valeurs du minuteur SIP
- Traitement des codes d'état de réponse
- Paramètres RTP
- Types de données utiles SDP
- Paramètres de prise en charge NAT

Paramètres SIP

Voice > SIP > SIP Parameters

Max Forward	Valeur maximale de transfert, comprise entre 1 et 255. La valeur par défaut est 70.
Max Redirection	Nombre de fois qu'un message d'invite peut être redirigé afin d'éviter une boucle infinie. La valeur par défaut est 5.
Max Auth	Nombre maximal de fois (de 0 à 255) qu'une demande peut être faite. La valeur par défaut est 2.
SIP User Agent Name	En-tête User-Agent utilisé dans les demandes sortantes. Si le champ est vide, l'en-tête n'est pas inclus. Extension macro de $A à $D correspondant à GPP_A à GPP_D autorisé. La valeur par défaut est $VERSION.
SIP Server Name	En-tête de serveur utilisé pour les réponses entrantes. La valeur par défaut est $VERSION.
SIP Reg User Agent Name	Nom de l'agent utilisateur à utiliser dans la demande REGISTER. Si cette valeur n'est pas spécifiée, le paramètre SIP User Agent Name est également utilisé pour la demande REGISTER. Par défaut, cette valeur n'est pas définie.

SIP Accept Language	En-tête de langage d'acceptation utilisé. Il n'existe pas de valeur par défaut (cela signifie que la SRP n'inclut pas cet en-tête). Si le champ est vide, l'en-tête n'est pas inclus.
DTMF Relay MIME Type	Type de protocole MIME utilisé dans un message SIP INFO pour signaler un événement DTMF. La valeur par défaut est application/dtmf-relay.
Remove Last Reg	Permet de supprimer le dernier enregistrement avant d'en enregistrer un nouveau si la valeur est différente. Sélectionnez yes ou no dans la liste déroulante. La valeur par défaut est no.
Use Compact Header	Permet d'utiliser des en-têtes SIP compacts dans les messages SIP sortants. Sélectionnez yes ou no dans la liste déroulante. Si le paramètre est défini sur yes, la SRP utilise les en-têtes SIP compacts dans les messages SIP sortants. S'il est défini sur no, la SRP utilise des en-têtes SIP normaux. Si les demandes SIP entrantes contiennent des en-têtes compacts, la SRP réutilise ces mêmes en-têtes pour générer la réponse, quelle que soit la configuration du paramètre Use Compact Header. Si les demandes SIP entrantes contiennent des en-têtes normaux, la SRP remplace ces en-têtes par des en-têtes compacts (s'ils sont définis par RFC 261) si le paramètre Use Compact Header est défini sur yes. La valeur par défaut est no.
Escape Display Name	Permet de ne pas afficher le nom. Sélectionnez yes si vous souhaitez que la SRP mette la chaîne (configurée dans le nom d'affichage) entre guillemets anglais pour les messages SIP sortants. Si le nom d'affichage comprend les signes " ou \, ces derniers seront transformés en \" et \\ entre guillemets. Sinon, sélectionnez no. La valeur par défaut est no.

RFC 2543 Call Hold	Configure le type de mise en attente : a:sendonly ou 0.0.0.0. La valeur par défaut est no ; n'utilisez pas la syntaxe 0.0.0.0 pour HOLD SDP, utilisez plutôt la syntaxe a:sendonly. Mark All AVT Packets S'il est réglé sur yes, le bit de marquage de tous les paquets de tonalité AVT (codés pour redondance) est configuré. S'il est réglé sur no, seul le bit marqueur du premier paquet est configuré pour chaque événement DTMF. La valeur par défaut est yes.
Mark all AVT Packets	S'il est réglé sur yes, le bit de marquage de tous les paquets de tonalité AVT (codés pour redondance) est configuré. S'il est réglé sur no, seul le bit marqueur du premier paquet est configuré pour chaque événement DTMF. La valeur par défaut est yes.
SIP TCP Port Min	Il spécifie le plus petit numéro de port TCP pouvant être utilisé pour les sessions SIP. La valeur par défaut est 5060.
SIP TCP Port Max	Il spécifie le plus grand numéro de port TCP pouvant être utilisé pour les sessions SIP. La valeur par défaut est 5080.

Valeurs du minuteur SIP

Voice > SIP > SIP Timer Values

SIP T1	Valeur RFC 3261 T1 (estimation RTT), comprise entre 0 et 64 secondes. La valeur par défaut est 0.5.
SIP T2	Valeur RFC 3261 T2 (intervalle de retransmission maximal pour les requêtes non-INVITE et les réponses INVITE), comprise entre 0 et 64 secondes. La valeur par défaut est 4.

SIP T4	Valeur RFC 3261 T4 (durée maximale de présence d'un message sur le réseau), comprise entre 0 et 64 secondes. La valeur par défaut est 5.
SIP Timer B	Valeur du délai d'expiration du message INVITE, comprise entre 0 et 64 secondes. La valeur par défaut est 32.
SIP Timer F	Valeur de temporisation non-INVITE pouvant s'étendre de 0 à 64 secondes. La valeur par défaut est 32.
SIP Timer H	Valeur de temporisation de la réponse finale H INVITE, qui peut s'étendre de 0 à 64 secondes. La valeur par défaut est 32.
SIP Timer D	Durée d'attente ACK, comprise entre 0 et 64 secondes. La valeur par défaut est 32.
SIP Timer J	Durée d'attente de la réponse Non-INVITE, comprise entre 0 et 64 secondes. La valeur par défaut est 32.
INVITE Expires	Valeur de l'en-tête Expires de la requête INVITE. Si vous saisissez 0, l'en-tête Expires n'est pas inclus dans la requête. La valeur par défaut est 240. Plage : 0–(2^{31}-1).
ReINVITE Expires	Valeur de l'en-tête Expires de la requête ReINVITE. Si vous saisissez 0, l'en-tête Expires n'est pas inclus dans la requête. La valeur par défaut est 30. Plage : 0–(2^{31}-1).
Reg Min Expires	Il indique le temps minimal autorisé avant l'expiration de l'enregistrement pour le proxy dans l'en-tête Expires ou en tant que paramètre de l'en-tête Contact. Si le proxy renvoie une valeur inférieure à ce paramètre, c'est cette valeur minimale qui sera utilisée. La valeur par défaut est 1.

Reg Max Expires	Il indique le temps minimal autorisé avant l'expiration de l'enregistrement par le proxy dans l'en-tête Min-Expires. Si le proxy renvoie une valeur supérieure à ce paramètre, c'est cette valeur maximale qui est utilisée. La valeur par défaut est 7200.
Reg Retry Intvl	Intervalle d'attente avant que la SRP n'effectue une nouvelle tentative d'enregistrement après le dernier échec. La valeur par défaut est 30.
Reg Retry Long Intvl	Lorsque l'enregistrement échoue avec un code de réponse SIP ne correspondant pas à Retry Reg RSC, la SRP patiente pendant l'intervalle indiqué avant d'effectuer une nouvelle tentative. Si cet intervalle est égal à 0, la SRP interrompt ses tentatives. Cette valeur doit être supérieure à la valeur Reg Retry Intvl non nulle. La valeur par défaut est 1200.

Traitement des codes d'état de réponse

Voice > SIP > Response Status Code Handling

SIT1 RSC	Code d'état de la réponse SIP pour la tonalité d'informations spéciales (SIT) appropriée. Par exemple, si vous définissez le SIT1RSC sur 404, lorsque l'utilisateur effectue un appel et qu'un code d'échec 404 est renvoyé, la tonalité SIT1 est émise. La tonalité de réorganisation ou de ligne occupée est émise pour tous les codes d'état d'échec de réponse de SIT1RSC à SIT4RSC.
SIT2 RSC	Code d'état de la réponse SIP au message INVITE pour lequel la tonalité SIT2 est émise.
SIT3 RSC	Code d'état de la réponse SIP au message INVITE pour lequel la tonalité SIT3 est émise.
SIT4 RSC	Code d'état de la réponse SIP au message INVITE pour lequel la tonalité SIT4 est émise.

Try Backup RSC	Code de réponse SIP qui effectue une nouvelle tentative auprès d'un serveur de sauvegarde pour la requête actuelle.
Retry Reg RSC	Intervalle d'attente avant que la SRP n'effectue une nouvelle tentative d'enregistrement après le dernier échec.

Paramètres RTP

Voice > SIP > RTP Parameters

RTP Port Min	Numéro de port minimal pour la transmission et la réception RTP. Les paramètres RTP Port Min et RTP Port Max définissent une plage contenant au moins 4 numéros de ports pairs, comme 100–106. La valeur par défaut est 16384.
RTP Port Max	Numéro de port maximal pour la transmission et la réception RTP. La valeur par défaut est 16482.
RTP Packet Size	Taille des paquets en secondes, comprise entre 0,01 et 0,16. Pour être correctes, ces valeurs doivent être des multiples de 0,01 seconde. La valeur par défaut est 0.030.
Max RTP ICMP Err	Nombre d'erreurs ICMP successives autorisées lors de la transmission des paquets RTP à l'homologue avant que la SRP ne mette fin à l'appel. Si la valeur est définie sur 0, la SRP ignore la limite d'erreurs ICMP. La valeur par défaut est 0.

RTCP Tx Interval	Intervalle d'envoi de rapports d'expéditeur RTCP sur une connexion active. Cet intervalle peut être compris entre 0 et 255 secondes. Pendant une connexion active, la SRP peut être programmée pour envoyer les paquets RTCP de composants sur la connexion. Chaque paquet de composants RTP, hormis le dernier, contient un rapport d'expéditeur (SR) et une description de la source (SDES). Le dernier paquet RTCP contient un paquet BYE supplémentaire. Chaque SR, hormis le dernier, contient exactement 1 RR (Receiver Report) ; le dernier SR ne contient pas de RR. Le SDES contient les identifiants CNAME, NAME et TOOL. Le CNAME est défini sur <User ID>@<Proxy>, NAME est défini sur <Display Name> (ou Anonymous si l'utilisateur bloque l'ID de l'appelant) et TOOL est défini sur fournisseur/matériel-plate-forme-logiciel-version (exemple : Cisco/srp5201.0.31 (b) ou Cisco/ srp5401.0.31 (b)). L'horodatage NTP utilisé dans la SR est un instantané de l'heure locale de la SRP et non de l'heure signalée par le serveur NTP. Si la SRP reçoit un RR d'un homologue, elle tente de calculer le délai de l'aller-retour et l'exprime alors sous la forme de la valeur <Call Round Trip Delay> (en millisecondes) sur la page Info > Voice. La valeur par défaut est 0.
No UDP Checksum	Sélectionnez yes si vous souhaitez que la SRP calcule le total de contrôle de l'en-tête UDP des messages SIP. Sinon, sélectionnez no. La valeur par défaut est no.

Stats In BYE	Détermine si la SRP comprend l'en-tête P-RTP-Stat ou la réponse dans un message BYE. Cet en-tête contient les statistiques RTP de l'appel en cours. Sélectionnez yes ou no dans la liste déroulante. Le format de l'en-tête P-RTP-Stat est le suivant : P-RTP-State: PS=<packets sent>,OS=<octets sent>,PR=<packets received>,OR=<octets received>,PL=<packets lost>,JI=<jitter in ms>,LA=<delay in ms>,DU=<call duration ins>,EN=<encoder>,DE=<decoder>. La valeur par défaut est yes.

Types de données utiles SDP

Voice > SIP > SDP Payload Types

NSE Dynamic Payload	Type de données utiles dynamiques NSE. La plage valide s'étend de 96 à 127. La valeur par défaut est 100.
AVT Dynamic Payload	Type de données utiles dynamiques AVT. La plage valide s'étend de 96 à 127. La valeur par défaut est 101.
INFOREQ Dynamic Payload	Type de données utiles dynamiques INFOREQ. Il n'y a pas de valeur par défaut.
G726r32 Dynamic Payload	Type de données utiles dynamiques G726r32. La valeur par défaut est 2.
G729b Dynamic Payload	Type de données utiles dynamiques G.729b. La plage valide s'étend de 96 à 127. La valeur par défaut est 99.
EncapRTP Dynamic Payload	Type de données utiles dynamiques EncapRTP. La valeur par défaut est 112.
RTP-Start-Loopback Dynamic Payload	Type de charge utile dynamique RTP-Start-Loopback. La valeur par défaut est 113.

Codec RTP-Start-Loopback 500	Codec de démarrage du bouclage RTP. Sélectionnez l'une des options suivantes : G711u, G711a, G726-32, G729a. La valeur par défaut est G711u.
NSE Codec Name	Nom du codec NSEdans le SDP. La valeur par défaut est NSE.
AVT Codec Name	Nom du codec AVT utilisé dans le SDP. La valeur par défaut est telephone-event.
G711u Codec Name	Nom du codec G.711u utilisé dans le SDP. La valeur par défaut est PCMU.
G711a Codec Name	Nom du codec G.711a utilisé dans le SDP. La valeur par défaut est PCMA.
G726r32 Codec Name	Nom du codec G.726-32 utilisé dans le SDP. La valeur par défaut est G726-32.
G729a Codec Name	Nom du codec G.729a utilisé dans le SDP. La valeur par défaut est G729a.
G729b Codec Name	Nom du codec G.729b utilisé dans le SDP. La valeur par défaut est G729ab.
EncapRTP Codec Name	Nom du codec EncapRTP utilisé dans le SDP. La valeur par défaut est EncapRTP.

Paramètres de prise en charge NAT

Voice > SIP > NAT Support Parameters

Handle VIA received	Si vous sélectionnez yes, la SRP traite le paramètre reçu dans l'en-tête VIA (cette valeur est insérée par le serveur dans une réponse à l'une de ses demandes). Si vous sélectionnez no, ce paramètre est ignoré. Sélectionnez **yes** ou **no** dans le menu déroulant. La valeur par défaut est no.

Handle VIA rport	Si vous sélectionnez yes, la SRP traite le paramètre de rapport dans l'en-tête VIA (cette valeur est insérée par le serveur dans une réponse à l'une de ses demandes). Si vous sélectionnez no, ce paramètre est ignoré. Sélectionnez **yes** ou **no** dans le menu déroulant. La valeur par défaut est no.
Insert VIA received	Permet d'insérer le paramètre reçu dans l'en-tête VIA des réponses SIP si les valeurs reçues par IP et VIA envoyées par IP diffèrent. Sélectionnez yes ou no dans le menu déroulant. La valeur par défaut est no.
Insert VIA rport	Permet d'insérer le paramètre dans l'en-tête VIA des réponses SIP si les valeurs reçues de l'IP et les valeurs VIA envoyées par IP diffèrent. Sélectionnez **yes** ou **no** dans le menu déroulant. La valeur par défaut est no.
Substitute VIA Addr	Permet d'utiliser les valeurs IP mappées par NAT : valeurs du port dans l'en-tête VIA. Sélectionnez yes ou no dans le menu déroulant. La valeur par défaut est no.
Send Resp To Src Port	Permet d'envoyer les réponses au port source de la requête et non aux valeurs VIA envoyées par port. Sélectionnez yes ou no dans le menu déroulant. La valeur par défaut est no.
STUN enable	Permet d'activer l'utilisation du STUN pour détecter le mappage NAT. Sélectionnez yes ou no dans le menu déroulant. La valeur par défaut est no.
STUN Test Enable	Si la fonctionnalité STUN Enable est activée et qu'un serveur STUN valide est disponible, la SRP peut effectuer une opération de détection du type NAT lorsqu'il démarre. Il contacte le serveur STUN configuré et le résultat de la recherche est consigné dans un en-tête Warning pour toutes les requêtes REGISTER suivantes. Si la SRP détecte un NAT symétrique ou un pare-feu symétrique, le mappage NAT est désactivé. La valeur par défaut est no.

STUN Server	Adresse IP ou nom de domaine complet du serveur STUN à contacter pour la détection du mappage NAT.
EXT IP	Adresse IP externe à substituer à l'adresse IP réelle de la SRP dans tous les messages SIP sortants. Si vous indiquez 0.0.0.0, aucune substitution d'adresse IP n'est effectuée. Si ce paramètre est défini, la SRP utilise cette adresse IP lorsqu'elle génère des messages SIP et SDP (si le mappage NAT est activé sur cette ligne). Cependant, les résultats du traitement des paramètres reçus STUN et VIA, s'ils sont disponibles, remplacent cette valeur configurée de manière statique. **REMARQUE** Cette option nécessite que vous ayez (1) une adresse IP statique de votre fournisseur d'accès à Internet et (2) un périphérique réseau avec un mécanisme NAT symétrique. Si la SRP est un périphérique réseau, la nouvelle demande obtient une réponse. La valeur par défaut est 0.0.0.0.
EXT RTP Port Min	Numéro de mappage du port externe du numéro RTP Port Min. Si cette valeur est différente de zéro, le numéro de port RTP dans tous les messages SIP sortants est substitué par la valeur de port correspondante dans la plage des ports RTP externes. Il n'existe aucune valeur par défaut.
NAT Keep Alive Intvl	Intervalle entre les messages de maintien de connexion du mappage NAT. La valeur par défaut est 15.

Page Provisioning

Utilisez la page Provisioning pour configurer différents profils et paramètres. Cette page comprend les sections suivantes :

- **Profil de configuration**
- **Mise à niveau du microprogramme**
- **Paramètres généraux**

Profil de configuration

Voice > Provisioning > Configuration Profile

Provision Enable	Commande toutes les actions de resynchronisation indépendamment des actions de mise à niveau des microprogrammes. Définissez-la sur Yes pour activer la configuration à distance. La valeur par défaut est Yes.
Resync On Reset	Déclenche une resynchronisation après chaque redémarrage, à l'exception des redémarrages causés par les mises à jour des paramètres et des mises à niveau des microprogrammes. La valeur par défaut est Yes.
Resync Random Delay	Valeur maximale d'un intervalle aléatoire pendant lequel le périphérique attend avant d'établir son contact initial avec le serveur de mise en service. Ce délai est efficace uniquement sur la tentative de configuration initiale qui suit le démarrage ou la réinitialisation du périphérique. Le délai est un nombre pseudo-aléatoire compris entre zéro et cette valeur. Ce paramètre est en unités de 20 secondes ; la valeur par défaut de 2 représente 40 secondes. Cette fonctionnalité est désactivée lorsque ce paramètre est défini sur zéro. Cette fonctionnalité peut être utilisée pour empêcher toute surcharge du serveur de mise en service lorsqu'un grand nombre de périphériques démarrent simultanément. La valeur par défaut est 2 (40 secondes).

Resync Periodic	Intervalle entre les resynchronisations périodiques avec le serveur de mise en service. Le minuteur de resynchronisation associé est actif uniquement après la première synchronisation réussie avec le serveur. Définissez ce paramètre sur zéro pour désactiver la resynchronisation périodique. La valeur par défaut est 3600 secondes.
Resync Error Retry Delay	Intervalle de tentatives de resynchronisation (en secondes) appliqué en cas d'échec de la resynchronisation. Le périphérique est équipé d'un minuteur de saisie des erreurs qui s'allume si la tentative de synchronisation précédente avec le serveur de mise en service échoue. Le périphérique attend que le minuteur effectue le décompte jusqu'à zéro pour recontacter le serveur. Ce paramètre est la valeur ajoutée initialement chargée dans le minuteur de saisie des erreurs. Si ce paramètre est défini sur zéro, le périphérique réessaye immédiatement de se synchroniser avec le serveur de mise en service à la suite de la tentative manquée. La valeur par défaut est 3600 secondes.
Forced Resync Delay	Délai maximal (en secondes) pendant lequel le SPA attend avant d'effectuer une resynchronisation. Le périphérique n'effectue pas de resynchronisation lorsqu'une de ses lignes téléphoniques est active. Dans la mesure où une resynchronisation peut prendre plusieurs secondes, il est souhaitable d'attendre que le périphérique soit inactif pendant une période prolongée avant de resynchroniser. Cela permet à un utilisateur de passer des appels successifs sans interruption. Le périphérique est équipé d'un minuteur qui lance le décompte lorsque toutes ses lignes deviennent inactives. Ce paramètre correspond à la valeur initiale du compteur. Les événements de resynchronisation sont retardés jusqu'à ce que ce compteur diminue jusqu'à zéro. La valeur par défaut est 14,400 secondes.

Resync From SIP	Permet le déclenchement d'une resynchronisation via un message SIP NOTIFY. La valeur par défaut est Yes.
Resync After Upgrade Attempt	Déclenche une resynchronisation après chaque tentative de mise à niveau des microprogrammes. La valeur par défaut est Yes.
Resync Trigger 1 Resync Trigger 2	Conditions configurables de déclenchement de la resynchronisation. Une resynchronisation est déclenchée lorsque l'équation de logique de ces paramètres est évaluée sur TRUE. La valeur par défaut est (vide).
Resync Fails On FNF	Indique si une réponse file-not-found du serveur de mise en service constitue une resynchronisation réussie ou défaillante. Une resynchronisation défaillante active le minuteur de resynchronisation des erreurs. La valeur par défaut est Yes.
Profile Rule	Ce paramètre est un script de profil qui est évalué à l'aide de la commande de resynchronisation de la mise en service. La commande est une opération TCP/IP et une URL associée. L'opération TCP/IP peut être TFTP, HTTP ou HTTPS. Si la commande n'est pas spécifiée, TFTP est supposé et l'adresse du serveur TFTP est obtenue via DHCP option 66. Dans l'URL, l'adresse IP ou le FQDN du serveur peut être spécifié. Le nom de fichier peut comprendre des macros, tels que $MA, qui s'étend à l'adresse MAC du périphérique. La valeur par défaut est /srp$PSN.cfg.
Profile Rule B: Profile Rule C: Profile Rule D:	Définissent les deuxième, troisième et quatrième commandes de resynchronisation et les URL de profil associées. Ces scripts de profil sont exécutés séquentiellement une fois l'opération principale de resynchronisation des règles de profil terminée. Si une resynchronisation est déclenchée et que la règle de profil est vide, les règles de profil B, C et D sont toujours évaluées et exécutées. La configuration par défaut est (vide).

Profile Name and Profile Region	Un serveur de mise en service peut stocker des données de chaîne dans ce paramètre, puis relire ces données en interrogeant le périphérique. Il ne remplit aucune autre fonction interne.
Log Resync Request Msg	Ce paramètre contient le message qui est envoyé au serveur syslog au début d'une tentative de resynchronisation. La valeur par défaut est $PN $MAC – Requesting resync $SCHEME://$SERVIP:$PORT$PATH.
Log Resync Success Msg	Message syslog publié lorsque vous avez terminé avec succès une tentative de resynchronisation. La valeur par défaut est $PN $MAC – Successful resync $SCHEME://$SERVIP:$PORT$PATH -- $ERR.
Log Resync Failure Msg	Message syslog publié après une tentative de resynchronisation défaillante. La valeur par défaut est $PN $MAC – Resync failed: $ERR.
Report Rule	URL de destination à laquelle les rapports de configuration sont envoyés. Ce paramètre a la même syntaxe que le paramètre Profile_Rule et se résout en une commande TCP/IP avec une URL associée. Un rapport de configuration est généré en réponse à un message SIP NOTIFY authentifié, avec Event: report. Le rapport est un fichier XML contenant le nom et la valeur de tous les paramètres de périphérique. Ce paramètre peut éventuellement contenir une clé de cryptage. Par exemple : [--key $K] tftp://ps.callhome.net/$MA/rep.xml.enc La configuration par défaut est (vide).

Mise à niveau du microprogramme

Voice > Provisioning > Firmware Upgrade

Upgrade Enable	Permet les opérations de mise à niveau du microprogramme indépendamment des actions de resynchronisation. La valeur par défaut est Yes.
Upgrade Error Retry Delay	L'intervalle pour réessayer la mise à niveau (en secondes) s'applique lorsque la mise à niveau échoue. Le périphérique dispose d'un temporisateur d'erreur de mise à niveau du microprogramme qui s'active après l'échec d'une tentative de cette mise à niveau. Le temporisateur est initialisé avec la valeur configurée dans ce paramètre. La prochaine tentative de mise à niveau du microprogramme sera effectuée lorsque le décompte de ce temporisateur arrivera à zéro. La valeur par défaut est 3600 secondes.
Downgrade Rev Limit	Applique une limite inférieure au numéro de version acceptable pendant une mise à niveau ou une rétrogradation du microprogramme. Le périphérique ne termine pas une opération de mise à niveau du microprogramme si la version du microprogramme n'est pas égale ou supérieure à ce paramètre. La valeur par défaut est (vide).
Upgrade Rule	Ce paramètre est un script de mise à niveau du microprogramme ayant une syntaxe identique à Profile_Rule. Définit les conditions de la mise à niveau et les adresses URL associées du microprogramme. La valeur par défaut est (vide).
Log Upgrade Request Msg	Le message syslog émis au début d'une tentative de mise à niveau du microprogramme. La valeur par défaut est $PN $MAC -- Requesting upgrade $SCHEME://$SERVIP:$PORT$PATH.
Log Upgrade Success Msg	Le message syslog émis après une tentative réussie de mise à niveau du microprogramme. La valeur par défaut est $PN $MAC -- Successful upgrade $SCHEME://$SERVIP:$PORT$PATH -- $ERR.

Log Upgrade Failure Msg	Le message syslog émis après l'échec d'une tentative de mise à niveau du microprogramme. La valeur par défaut $PN $MAC -- Upgrade failed: $ERR.
License Keys	Ce champ n'est actuellement pas utilisé par la SRP500.

Paramètres généraux

Voice > Provisioning > General Purpose Parameters

GPP A to GPP P	Paramètres de configuration généraux. Ces paramètres peuvent être utilisés en tant que variables dans les règles de mise en service et mise à niveau. Ils sont référencés en ajoutant le nom de la variable avec un caractère '$', comme $GPP_A. La configuration par défaut est (vide).

Page Regional

Utilisez la page Regional pour localiser votre système avec les paramètres régionaux appropriés. Les sections suivantes apparaissent sur la page **Voice > Regional**.

- **Tonalités de progression d'appel**
- **Modèles de sonneries distinctes**
- **Modèles distincts de tonalité d'appel en attente**
- **Noms distincts de modèles de CWT/sonnerie**
- **Valeurs de minuteur de contrôle**
- **Codes d'activation du service vertical**
- **Codes d'annonce du service vertical**
- **Codes de sélection des codecs des appels vers l'extérieur**
- **Miscellaneous**

Définition des scripts de sonnerie, de cadence et de tonalité

Pour définir des modèles de sonnerie et de tonalité, la SRP utilise le concept des scripts. L'exemple suivant définit comment créer des scripts de cadence (CadScripts), des scripts de fréquence (FreqScripts) et des scripts de tonalité (ToneScripts).

CadScript

Mini-script de 127 caractères maximum qui spécifie les paramètres de cadence d'un signal.

Syntaxe : $S_1[;S_2]$, où :
$S_i=D_i(on_i,1/off_i,1[,on_{i,2}/off_{i,2}[,on_{i,3}/off_{i,3}[,on_{i,4}/off_{i,4}[,on_{i,5}/off_{i,5},on_{i,6}/off_{i,6}]]]]])$ et est connu en tant que section, $on_{i,j}$ et $off_{i,j}$ représentent la durée d'activation/de désactivation en secondes d'un segment et i = 1 ou 2 et j = 1 à 6. D_i représente la durée totale de la section en secondes. Toutes les durées peuvent posséder jusqu'à trois décimales pour fournir une résolution à 1 ms. Le caractère générique « * » représente une durée infinie. Les segments d'une section sont émis dans l'ordre et répétés jusqu'à la fin de la durée totale.

Exemple 1 : 60(2/4)

```
Number of Cadence Sections = 1Cadence Section 1: Section Length = 60 sNumber
of Segments = 1Segment 1: On=2s, Off=4sTotal Ring Length = 60s
```

Exemple 2 : sonnerie distincte (court, court, court, long) : 60(.2/.2,.2/.2,.2/.2,1/4)

```
Number of Cadence Sections = 1Cadence Section 1: Section Length = 60sNumber
of Segments = 4Segment 1: On=0.2s, Off=0.2sSegment 2: On=0.2s,
Off=0.2sSegment 3: On=0.2s, Off=0.2sSegment 4: On=1.0s, Off=4.0sTotal Ring
Length = 60s
```

FreqScript

Mini-script de 127 caractères maximum qui spécifie les paramètres de fréquence et de niveau d'une tonalité.

Syntaxe : $F_1@L_1[,F_2@L_2[,F_3@L_3[,F_4@L_4[,F_5@L_5[,F_6@L_6]]]]]$
où F_1–F_6 représente la fréquence en Hz (entiers non signés uniquement) et L_1–L_6 sont les niveaux correspondants en dBm, avec une décimale au maximum. Les espaces blancs avant et après la virgule sont autorisées (mais non recommandés).

Exemple 1 : tonalité d'appel en attente : 440@-10

```
Number of Frequencies = 1
    Frequency 1 = 440 Hz at –10 dBm
```

Exemple 2 : tonalité : 350@-19,440@-19

```
Number of Frequencies = 2
    Frequency 1 = 350 Hz at –19 dBm
    Frequency 2 = 440 Hz at –19 dBm
```

ToneScript

Mini-script de 127 caractères maximum qui spécifie les paramètres de fréquence, de niveau et de cadence d'une tonalité de progression d'appel. Il peut comprendre jusqu'à 127 caractères.

Syntaxe : FreqScript;Z_1[;Z_2].
La section Z_1 est similaire à la section S_1 d'un CadScript, sauf que chaque segment activé ou désactivé est suivi d'un paramètre de composants de fréquence : Z_1 = D_1($on_{i,1}$/$off_{i,1}$/$f_{i,1}$[,$on_{i,2}$/$off_{i,2}$/$f_{i,2}$ [,$on_{i,3}$/$off_{i,3}$/$f_{i,3}$[,$on_{i,4}$/$off_{i,4}$/$f_{i,4}$[,oni,5/$off_{i,5}$/$f_{i,5}$[,$on_{i,6}$/$off_{i,6}$/fi,6]]]]]), où fi,j = n_1[+n_2]+n_3[+n_4[+n_5[+n_6]]]] et 1 < n_k < 6 indique quels composants de fréquence du FreqScript sont utilisés dans ce segment ; si plusieurs composants de fréquence sont utilisés dans un segment, les composants sont additionnés.

Exemple 1 : tonalité : 350@-19,440@-19;10(*/0/1+2)

```
Number of Frequencies = 2
    Frequency 1 = 350 Hz at –19 dBm
    Frequency 2 = 440 Hz at –19 dBm
Number of Cadence Sections = 1
    Cadence Section 1: Section Length = 10 s
    Number of Segments = 1
        Segment 1: On=forever, with Frequencies 1 and 2
Total Tone Length = 10s
```

Exemple 2 : tonalité saccadée : 350@-19,440@-19;2(.1/.1/1+2);10(*/0/1+2)

```
Number of Frequencies = 2
    Frequency 1 = 350 Hz at –19 dBm
    Frequency 2 = 440 Hz at –19 dBm
Number of Cadence Sections = 2
    Cadence Section 1: Section Length = 2s
        Number of Segments = 1
            Segment 1: On=0.1s, Off=0.1s with Frequencies 1 and 2
    Cadence Section 2: Section Length = 10s
        Number of Segments = 1
            Segment 1: On=forever, with Frequencies 1 and 2
Total Tone Length = 12s
```

Tonalités de progression d'appel

Voice > Regional > Call ProgressTones

Dial Tone	Invite l'utilisateur à saisir un numéro de téléphone. La tonalité de réorganisation est émise automatiquement après expiration de Dial Tone ou de l'une de ses alternatives. La valeur par défaut est 350@-19,440@-19;10(*/0/1+2).
Second Dial Tone	Alternative à la tonalité de numérotation lorsque l'utilisateur effectue un appel à trois. La valeur par défaut est 420@-19,520@-19;10(*/0/1+2).
Outside Dial Tone	Alternative à la tonalité de numérotation. Invite l'utilisateur à composer un numéro de téléphone externe, par opposition aux postes internes. Elle est déclenchée par une virgule (,) dans le plan de numérotation. La valeur par défaut est 420@-19;10(*/0/1).
Prompt Tone	Invite l'utilisateur à saisir un numéro de téléphone pour le renvoi d'appel. La valeur par défaut est 520@-19,620@-19;10(*/0/1+2).
Busy Tone	Cette tonalité est émise lorsqu'un code 486 RSC est reçu lors d'un appel sortant. La valeur par défaut est 480@-19,620@-19;10(.5/.5/1+2).
Reorder Tone	Cette tonalité est émise lorsqu'un appel sortant a échoué ou lorsque le poste distant raccroche au cours d'un appel établi. La tonalité de réorganisation est émise automatiquement après expiration de Dial Tone ou de l'une de ses alternatives. La valeur par défaut est 480@-19,620@-19;10(.25/.25/1+2).
Off Hook WarningTone	Cette tonalité est émise lorsque l'appelant n'a pas correctement replacé le combiné sur son support. Le décrochage avec tonalité d'avertissement se produit lorsque la tonalité de réorganisation expire. La valeur par défaut est 480@10,620@0;10(.125/.125/1+2).
Ring Back Tone	Cette tonalité est émise lors d'un appel sortant lorsque le poste distant sonne. La valeur par défaut est 440@-19,480@-19;*(2/4/1+2).

Ring Back 2 Tone	Votre SRP émet cette tonalité de rappel au lieu de Ring Back Tone si l'appelé émet une réponse SIP 182 sans SDP à la demande INVITE sortante. La valeur par défaut est identique à celle de Ring Back Tone hormis la cadence qui est de 1 s en marche et 1 s en arrêt. La valeur par défaut est 440@-19,480@-19;*(1/1/1+2).
Confirm Tone	Tonalité brève qui indique à l'utilisateur que la dernière valeur saisie a été acceptée. La valeur par défaut est 600@-16; 1(.25/.25/1).
SIT1 Tone	Alternative à la tonalité de réorganisation émise en cas d'erreur lorsqu'un appelant effectue un appel sortant. Le code RSC permettant de déclencher cette tonalité peut être configuré sur l'écran SIP. La valeur par défaut est 985@-16,1428@-16,1777@ 16;20(.380/0/1,.380/0/2,.380/0/3,0/4/0).
SIT2 Tone	Alternative à la tonalité de réorganisation émise en cas d'erreur lorsqu'un appelant effectue un appel sortant. Le code RSC permettant de déclencher cette tonalité peut être configuré sur l'écran SIP. La valeur par défaut est 914@-16,1371@-16,1777@ 16;20(.274/0/ 1,.274/0/2,.380/0/3,0/4/0).
SIT3 Tone	Alternative à la tonalité de réorganisation émise en cas d'erreur lorsqu'un appelant effectue un appel sortant. Le code RSC permettant de déclencher cette tonalité peut être configuré sur l'écran SIP. La valeur par défaut est 914@-16,1371@-16,1777@-16;20(.380/0/ 1,.380/0/2,.380/0/3,0/4/0).
SIT4 Tone	Alternative à la tonalité de réorganisation émise en cas d'erreur lorsqu'un appelant effectue un appel sortant. Le code RSC permettant de déclencher cette tonalité peut être configuré sur l'écran SIP. La valeur par défaut est 985@-16,1371@-16,1777@-16;20(.380/0/1,.274/0/2,.380/0/3,0/4/0).

MWI Dial Tone	Cette tonalité est émise à la place de la tonalité de numérotation lorsque des messages non écoutés sont présents dans la messagerie de l'appelant. La valeur par défaut est : 350@-19,440@-19;2(.1/.1/1+2);10(*/0 1+2).
Cfwd Dial Tone	Cette tonalité est émise lorsque tous les appels sont transférés. La valeur par défaut est : 350@-19,440@-19;2(.2/.2/1+2);10(*/0/1+2).
Holding Tone	Cette tonalité informe l'appelant local que le poste distant a placé son appel en attente. La valeur par défaut est 600@-19*(.1/.1/1,.1/.1/1,.1/9.5/1).
Conference Tone	Cette tonalité est émise à toutes les parties lorsqu'une conférence téléphonique à trois est en cours. La valeur par défaut est 350@-19;20(.1/.1/1,.1/9.7/1).
Secure Call Indication Tone	Cette tonalité est émise lorsqu'un appel est passé avec succès en mode sécurisé. Elle doit être émise de manière brève (moins de 30 secondes) et à un volume réduit (moins de -19 dBm) afin de ne pas perturber la conversation. La valeur par défaut est 397@-19,507@-19;15(0/2/0,.2/.1/1,.1/2.1/2).
Feature Invocation Tone	Cette tonalité est émise lorsqu'une fonctionnalité est mise en place. La valeur par défaut est 350@-16;*(.1/.1/1).

Modèles de sonneries distinctes

Voice > Regional > Distinctive Ring Patterns

Ring1 Cadence	Script de cadence de la sonnerie distincte 1. La valeur par défaut est 60(2/4).
Ring2 Cadence	Script de cadence de la sonnerie distincte 2. La valeur par défaut est 60(.8/.4,.8/4).
Ring3 Cadence	Script de cadence de la sonnerie distincte 3. La valeur par défaut est 60(.4/.2,.4/.2,.8/4).

Ring4 Cadence	Script de cadence de la sonnerie distincte 4. La valeur par défaut est 60(.3/.2,1/.2,.3/4).
Ring5 Cadence	Script de cadence de la sonnerie distincte 5. La valeur par défaut est 1(.5/.5).
Ring6 Cadence	Script de cadence de la sonnerie distincte 6. La valeur par défaut est 60(.2/.4,.2/.4,.2/4).
Ring7 Cadence	Script de cadence de la sonnerie distincte 7. La valeur par défaut est 60(.4/.2,.4/.2,.4/4).
Ring8 Cadence	Script de cadence de la sonnerie distincte 8. La valeur par défaut est 60(0.25/9.75).

Modèles distincts de tonalité d'appel en attente

Voice > Regional > Distinctive Call Waiting Tone Patterns

CWT1 Cadence	Script de cadence pour la tonalité distincte d'appel en attente CWT 1. La valeur par défaut est 30(.3/9.7).
CWT2 Cadence	Script de cadence pour la tonalité distincte d'appel en attente CWT 2. La valeur par défaut est 30(.1/.1,.1/9.7).
CWT3 Cadence	Script de cadence pour la tonalité distincte d'appel en attente CWT 3. La valeur par défaut est 30(.1/.1,.1/.1,.1/9.7).
CWT4 Cadence	Script de cadence pour la tonalité distincte d'appel en attente CWT 4. La valeur par défaut est 30(.3/.1.1/.1,.1/9.3).
CWT5 Cadence	Script de cadence pour la tonalité distincte d'appel en attente CWT 5. La valeur par défaut est 1(.5/.5).
CWT6 Cadence	Script de cadence pour la tonalité distincte d'appel en attente CWT 6. La valeur par défaut est 30(.3/.1,.3/.1,.1/9,1).

CWT7 Cadence	Script de cadence pour la tonalité distincte d'appel en attente CWT 7. La valeur par défaut est 30(.3/.1,.3/.1,.1/9,3).
CWT8 Cadence	Script de cadence pour la tonalité distincte d'appel en attente CWT 8. La valeur par défaut est 2.3(.3/2).

Noms distincts de modèles de CWT/sonnerie

IMPORTANTE. La sonnerie et les tonalités d'appel en attente ne fonctionnent pas de la même manière sur tous les téléphones. Lors de la configuration des tonalités, tenez compte des recommandations suivantes :

- Sélectionnez en premier la forme d'onde, la fréquence et la tension de la sonnerie.
- Si la cadence de votre sonnerie n'est pas conforme à vos attentes, ou si votre téléphone ne sonne pas, remplacez la forme d'onde, la fréquence et la tension de votre sonnerie par les valeurs suivantes :
  - Forme d'onde de la sonnerie : sinusoïdale
  - Fréquence de sonnerie : 25
  - Tension d'appel : 80 V CC

Voice > Regional > Distinctive Ring/CWT Pattern Names

Ring1 Name	Nom figurant dans l'en-tête Alert-Info du message INVITE permettant de sélectionner une sonnerie et une tonalité d'appel en attente distinctes pour l'appel entrant. La valeur par défaut est Bellcore-r1.
Ring2 Name	Nom figurant dans l'en-tête Alert-Info du message INVITE permettant de sélectionner une sonnerie et une tonalité d'appel en attente 2 distinctes pour l'appel entrant. La valeur par défaut est Bellcore-r2.

Ring3 Name	Nom figurant dans l'en-tête Alert-Info du message INVITE permettant de sélectionner une sonnerie et une tonalité d'appel en attente 3 distinctes pour l'appel entrant. La valeur par défaut est Bellcore-r3.
Ring4 Name	Nom figurant dans l'en-tête Alert-Info du message INVITE permettant de sélectionner une sonnerie et une tonalité d'appel en attente 4 distinctes pour l'appel entrant. La valeur par défaut est Bellcore-r4.
Ring5 Name	Nom figurant dans l'en-tête Alert-Info du message INVITE permettant de sélectionner une sonnerie et une tonalité d'appel en attente 5 distinctes pour l'appel entrant. La valeur par défaut est Bellcore-r5.
Ring6 Name	Nom figurant dans l'en-tête Alert-Info du message INVITE permettant de sélectionner une sonnerie et une tonalité d'appel en attente 6 distinctes pour l'appel entrant. La valeur par défaut est Bellcore-r6.
Ring7 Name	Nom figurant dans l'en-tête Alert-Info du message INVITE permettant de sélectionner une sonnerie et une tonalité d'appel en attente 7 distinctes pour l'appel entrant. La valeur par défaut est Bellcore-r7.
Ring8 Name	Nom figurant dans l'en-tête Alert-Info du message INVITE permettant de sélectionner une sonnerie et une tonalité d'appel en attente 8 distinctes pour l'appel entrant. La valeur par défaut est Bellcore-r8.
Ring Waveform	Forme d'onde du signal de la sonnerie. Vous pouvez sélectionner Sinusoid ou Trapezoid. La valeur par défaut est Trapezoid.
Ring Frequency	Fréquence du signal de la sonnerie. Les valeurs valides sont comprises entre 10 et 100 Hz. La valeur par défaut est 20.

Ring Voltage	Tension de la sonnerie. Les choix possibles sont compris entre **60 et 90** (V). La valeur par défaut est 85.
CWT Frequency	Script de fréquence de la tonalité de mise en attente. Cette tonalité sert de base à toutes les tonalités d'appel en attente distinctes. La valeur par défaut est 440@-10.
Synchronized Ring	Si cette option est définie sur Yes, lorsque la SRP est appelée, toutes les lignes sonnent en même temps (comme c'est le cas pour une ligne PSTN standard). Lorsqu'une ligne répond, les autres arrêtent de sonner. La valeur par défaut est no.

Valeurs de minuteur de contrôle

Voice > Regional > Control Timer Values (sec)

Hook Flash Timer Min	Durée minimale de combiné raccroché avant que le décrochage ne soit considéré comme un actionnement du crochet commutateur. En dessous de cette durée, l'événement combiné raccroché est ignoré. Intervalle : De 0,1 à 0,4 secondes. La valeur par défaut est 0.1.
Hook Flash Timer Max	Durée maximale de combiné raccroché avant que le décrochage ne soit considéré comme un actionnement du crochet commutateur. Cette durée dépassée, l'événement combiné raccroché est traité comme tel (et non comme un événement d'actionnement du crochet commutateur). Intervalle : De 0,4 à 1,6 secondes. La valeur par défaut est 0.9.
Callee On Hook Delay	Le téléphone doit être raccroché pendant cette durée, en secondes, avant que la SRP n'arrête l'appel entrant en cours. Cela ne s'applique pas aux appels sortants. Intervalle : de 0 à 255 secondes. La valeur par défaut est 0.

Reorder Delay	Délai après que le poste distant ait raccroché et avant l'émission de la tonalité de réorganisation. 0 = émission immédiate, inf = aucune émission. Intervalle : de 0 à 255 secondes. La valeur par défaut est 5.
Call Back Expires	Délai d'expiration en secondes de l'activation de l'option de rappel. Intervalle : de 0 à 65535 secondes. La valeur par défaut est 1800.
Call Back Retry Intvl	Intervalle en secondes avant une nouvelle tentative de rappel. Intervalle : de 0 à 255 secondes. La valeur par défaut est 30.
Call Back Delay	Délai après réception de la première réponse SIP 18x avant de faire sonner le poste distant. Si une réponse de ligne occupée est reçue durant ce délai, la SRP considère toujours l'appel comme ayant échoué et poursuit ses tentatives. La valeur par défaut est 0.5.
Internal VMWI Refresh Intvl	Intervalle entre les actualisations VMWI du CPE. La valeur par défaut est 0.
Interdigit Long Timer	Long dépassement du délai imparti entre la saisie des chiffres pendant la numérotation. Les valeurs du temporisateur inter-chiffres sont utilisées par défaut lors de la numérotation. Le paramètre Interdigit_Long_Timer est utilisé après n'importe quel chiffre, si toutes les séquences valides du plan de numérotation ne correspondent pas au numéro composé. Intervalle : de 0 à 64 secondes. La valeur par défaut est 10.
Interdigit Short Timer	Court dépassement du délai imparti entre la saisie des chiffres pendant la numérotation. Le paramètre Interdigit_Short_Timer est utilisé après n'importe quel chiffre, si le numéro composé correspond à au moins une séquence du plan de numérotation. Mais plus de chiffres composés peuvent faire correspondre le numéro à d'autres séquences incomplètes pour le moment. Intervalle : de 0 à 64 secondes. La valeur par défaut est 3.

CPC Delay	Délai en secondes après que l'appelant a raccroché, lorsque la SRP supprime la tension des fils de pointe et de nuque de l'équipement connecté de la partie appelée. La plage est comprise entre 0 et 255 secondes. Cette fonctionnalité est utilisée généralement par l'appelant pour la supervision de la réponse afin de signaler à l'équipement connecté le moment où l'appel est connecté (le système distant a décroché) ou déconnecté (le système distant a raccroché). Cette fonctionnalité doit être désactivée pour la partie appelée (autrement dit, en utilisant la même polarité pour l'état de connexion et d'inactivité). La fonctionnalité CPC doit être utilisée à la place. Si la fonctionnalité CPC n'est pas activée, la tonalité de réorganisation est émise après un délai configuré. Si la fonctionnalité CPC est activée, la tonalité est émise quand la tension des fils de pointe et de nuque est rétablie. La résolution est de 1 seconde. La plage par défaut est 2.
CPC Duration	Durée en secondes pendant laquelle la tension des fils de pointe et de nuque est arrêtée une fois que l'appelant a raccroché. Puis, la tension des fils de pointe et de nuque est rétablie et la tonalité est émise si l'équipement connecté est encore décroché. La fonctionnalité CPC est désactivée si cette valeur est définie sur 0. Plage : de 0 à 1 000 secondes. La résolution est de 0,001 seconde. La valeur par défaut est 0 (CPC désactivée).

Codes d'activation du service vertical

Les codes d'activation du service vertical sont ajoutés automatiquement au plan de numérotation. Il n'est pas nécessaire de les inclure dans le plan de numérotation, bien qu'il n'en résulte aucun dommage s'ils sont inclus.

Voice > Regional > Vertical Service Activation Codes

Call Return Code	Appelle le dernier appelant. La valeur par défaut est *69.
Call Redial Code	Rappelle le dernier numéro composé. La valeur par défaut est *07.

Blind Transfer Code	Ce code permet d'initier un transfert aveugle de l'appel en cours vers le poste indiqué à la suite du code d'activation. La valeur par défaut est *98.
Call Back Act Code	Ce code permet d'initier un rappel lorsque le dernier appel sortant n'est pas occupé. La valeur par défaut est *66.
Call Back Deact Code	Ce code permet d'annuler un rappel. La valeur par défaut est *86.
Call Back Act Busy Code	Initie un rappel lorsque le dernier appel sortant est occupé. La valeur par défaut est *05.
Cfwd All Act Code	Permet de transférer tous les appels vers le poste indiqué à la suite du code d'activation. La valeur par défaut est *72.
Cfwd All Deact Code	Permet d'annuler le transfert de tous les appels. La valeur par défaut est *73.
Cfwd Busy Act Code	Permet de transférer les appels occupés vers le poste indiqué à la suite du code d'activation. La valeur par défaut est *90.
Cfwd Busy Deact Code:	Permet d'annuler le transfert des appels occupés. La valeur par défaut est *91.
Cfwd No Ans Act Code	Permet de transférer les appels sans réponse vers le poste indiqué à la suite du code d'activation. La valeur par défaut est *92.
Cfwd No Ans Deact Code	Permet d'annuler le transfert des appels sans réponse. La valeur par défaut est *93.
Cfwd Last Act Code	Transfère les derniers appels entrants ou sortants vers le poste indiqué à la suite du code d'activation. La valeur par défaut est *63.
Cfwd Last Deact Code	Annule le renvoi des derniers appels entrants ou sortants. La valeur par défaut est *83.
Block Last Act Code	Bloque le dernier appel entrant. La valeur par défaut est *60.
Block Last Deact Code	Annule le blocage du dernier appel entrant. La valeur par défaut est *80.

Accept Last Act Code	Permet d'accepter le dernier appel sortant. Il permet l'émission de la sonnerie d'appel lorsque la fonctionnalité Ne pas déranger ou l'option de renvoi de tous les appels est activée. La valeur par défaut est *64.
Accept Last Deact Code	Annule le code d'acceptation du dernier appel sortant. La valeur par défaut est *84.
CW Act Code	Permet d'activer la mise en attente de tous les appels. La valeur par défaut est *56.
CW Deact Code	Permet de désactiver la mise en attente de tous les appels. La valeur par défaut est *57.
CW Per Call Act Code	Permet d'activer la mise en attente de l'appel suivant. La valeur par défaut est *71.
CW Per Call Deact Code	Permet de désactiver la mise en attente de l'appel suivant. La valeur par défaut est *70.
Block CID Act Code	Permet de bloquer l'ID de l'appelant pour tous les appels sortants. La valeur par défaut est *67.
Block CID Deact Code	Permet d'annuler le blocage de l'ID de l'appelant pour tous les appels sortants. La valeur par défaut est *68.
Block CID Per Call Act Code	Permet de bloquer l'ID de l'appelant pour l'appel sortant suivant. La valeur par défaut est *81.
Block CID Per Call Deact Code	Permet d'annuler le blocage de l'ID de l'appelant pour l'appel sortant suivant. La valeur par défaut est *82.
Block ANC Act Code	Permet de bloquer tous les appels anonymes. La valeur par défaut est *77.
Block ANC Deact Code	Permet d'annuler le blocage de tous les appels anonymes. La valeur par défaut est *87.
DND Act Code	Permet d'activer la fonctionnalité Ne pas déranger. La valeur par défaut est *78.
DND Deact Code	Permet de désactiver la fonctionnalité Ne pas déranger. La valeur par défaut est *79.

CID Act Code	Autorise la génération de l'identifiant de l'appelant. La valeur par défaut est *65.
CID Deact Code	Désactive la génération de l'identifiant de l'appelant. La valeur par défaut est *85.
CWCID Act Code	Active l'appel en attente et la génération de l'identifiant de l'appelant. La valeur par défaut est *25.
CWCID Deact Code	Désactive l'appel en attente et la génération de l'identifiant de l'appelant. La valeur par défaut est *45.
Dist Ring Act Code	Active la fonctionnalité de sonnerie distincte. La valeur par défaut est *26.
Dist Ring Deact Code	Désactive la fonctionnalité de sonnerie distincte. La valeur par défaut est *46.
Speed Dial Act Code	Attribue un numéro abrégé. La valeur par défaut est *74.
Paging Code	Utilisé pour la radiomessagerie d'autres clients du groupe. La valeur par défaut est *96.
Secure All Call Act Code	Permet de sécuriser tous les appels sortants. La valeur par défaut est *16.
Secure No Call Act Code	Permet de ne sécuriser aucun appel sortant. La valeur par défaut est *17.
Secure One Call Act Code	Permet de sécuriser l'appel sortant suivant. (Redondant si tous les appels sortants sont sécurisés par défaut.) La valeur par défaut est *18.
Secure One Call Deact Code	Permet de ne pas sécuriser l'appel sortant suivant. (Redondant si tous les appels sortants ne sont pas sécurisés par défaut.) La valeur par défaut est *19.
Conference Act Code	Si ce code est précisé, l'utilisateur doit le saisir avant de composer le numéro de la troisième personne participant à la conférence téléphonique. Saisissez le code de la conférence téléphonique.
Attn-Xfer Act Code	Si ce code est précisé, l'utilisateur doit le saisir avant de composer le numéro de la troisième personne pour le transfert d'appel. Saisissez le code du transfert d'appel.

Modem Line Toggle Code	Fait basculer la ligne sur un modem. La valeur par défaut est *99. Le mode Pass-through du modem ne peut être déclenché qu'en composant ce code à l'avance.
FAX Line Toggle Code	Fait basculer la ligne sur un télécopieur. La valeur par défaut est #99.
Media Loopback Code	Utilisez la fonctionnalité pour le bouclage multimédia. La valeur par défaut est *03.
Referral Services Codes	Ces codes indiquent à la SRP quelle opération effectuer lorsque l'utilisateur place l'appel en cours en attente et écoute la deuxième tonalité de numérotation. Plusieurs codes étoile peuvent être configurés dans ce paramètre, tels que *98 ou *97|*98|*123, etc. La longueur maximale totale est de 79 caractères. Ce paramètre est utilisé lorsque l'utilisateur place l'appel en cours en attente (par crochet commutateur) et écoute la deuxième tonalité de numérotation. Chaque code * (astérisque) (et le numéro cible valide suivant selon le plan de numérotation actuel) saisi lors de la deuxième tonalité déclenche la réalisation par la SRP d'un transfert aveugle vers le numéro cible ajouté par le code * de service. Par exemple, lorsque l'utilisateur compose le code *98, la SRP émet une tonalité spéciale appelée tonalité d'invite en attendant que l'utilisateur entre un numéro cible (qui est vérifié conformément au plan de numérotation comme lors d'une numérotation normale). Une fois le numéro complet saisi, la SRP envoie un message REFER aveugle à l'interlocuteur en attente, avec la cible Refer-To correspondant à *98 target_number. Cette fonctionnalité permet à la SRP de transférer l'appel à un serveur d'application afin de poursuivre le traitement, comme le parcage d'appels par exemple. Les codes * ne doivent pas entrer en conflit avec les autres codes de service vertical traités en interne par la SRP. Vous pouvez supprimer le code * correspondant que vous ne souhaitez pas que la SRP traite.

Feature Dial Services Codes	Ces codes indiquent à la SRP quelle opération effectuer lorsque l'utilisateur écoute la première ou la deuxième tonalité de numérotation. Plusieurs codes étoile peuvent être configurés dans ce paramètre, tels que *72 ou *72|*74|*67|*82, etc. La longueur maximale totale est de 79 caractères. Ce paramètre s'applique lorsque l'utilisateur entend une tonalité (première ou deuxième tonalité). Le code * (et le numéro cible valide suivant selon le plan de numérotation actuel) saisi lors de la tonalité déclenche l'appel par la SRP du numéro cible ajouté par le code *. Par exemple, une fois que l'utilisateur a composé *72, la SRP émet une tonalité spéciale appelée « Tonalité d'invite » jusqu'à ce que l'utilisateur entre un numéro de destination valide. Lorsqu'un numéro complet est saisi, la SRP envoie un message INVITE vers *72 target_number comme lors d'un appel normal. Cette fonctionnalité permet au proxy de traiter des fonctionnalités telles que le transfert d'appel (*72) ou le blocage de l'ID de l'appelant (*67). Les codes * ne doivent pas entrer en conflit avec les autres codes de service vertical traités en interne par la SRP. Vous pouvez supprimer le code * correspondant que vous ne souhaitez pas que la SRP traite. Vous pouvez ajouter un paramètre à chaque code étoile dans Features Dial Services Codes afin d'indiquer la tonalité à émettre après la saisie du code étoile, tel que *72‘c‘|*67‘p‘ par exemple. La liste ci-dessous indique les paramètres de tonalité autorisés (notez l'utilisation de guillemets ouverts sans espaces autour du paramètre) ‘c‘ = <Tonalité Cfwd> ‘d‘ = <Tonalité> ‘m‘ = <Tonalité MWI> ‘o‘ = <Tonalité externe> ‘p‘ = <Tonalité d'invite> ‘s‘ = <Tonalité secondaire> ‘x‘ = aucune tonalité, le x correspond à n'importe quel chiffre non utilisé ci-dessus. Si aucun paramètre de tonalité n'est indiqué, la SRP émet une tonalité d'invite par défaut. Si le code étoile n'est pas suivi par un numéro de téléphone, tel que *73 pour annuler le transfert d'appel, ne l'incluez pas dans ce paramètre. Dans ce cas, ajoutez simplement le code * dans le plan de numérotation et la SRP envoie un message INVITE *73@.... comme d'habitude lorsque l'utilisateur compose *73.’

Codes d'annonce du service vertical

Voice > Regional > Vertical Service Announcement Codes

Service Annc Base Number	Numéro de base des annonces de service. Par défaut, cette valeur n'est pas définie.
Service Annc Extension Codes	Codes d'extension des annonces de service. Par défaut, cette valeur n'est pas définie.

Codes de sélection des codecs des appels vers l'extérieur

Voice > Regional > Outbound Call Codec Selection Codes

Prefer G711u Code	Composez le préfixe pour faire de G.711u le codec préféré pour l'appel. La valeur par défaut est *017110.
Force G711u Code	Composez le préfixe pour faire de G.711u le seul codec qui peut être utilisé pour l'appel. La valeur par défaut est *027110.
Prefer G711a Code	Composez le préfixe pour faire de G.711a le codec préféré pour l'appel. La valeur par défaut est *017111.
Force G711a Code	Composez le préfixe pour faire de G.711a le seul codec qui peut être utilisé pour l'appel. La valeur par défaut est *027111.
Prefer G726r32 Code	Composez le préfixe pour faire de G.726r32 le codec préféré pour l'appel. La valeur par défaut est *0172632.
Force G726r32 Code	Composez le préfixe pour faire de G.726r32 le seul codec qui peut être utilisé pour l'appel. La valeur par défaut est *0272632.
Prefer G729a Code	Composez le préfixe pour faire de G.729a le codec préféré pour l'appel. La valeur par défaut est *01729.

Force G729a Code	Composez le préfixe pour faire de G.729a le seul codec qui peut être utilisé pour l'appel. La valeur par défaut est *02729.

Miscellaneous

Voice > Regional > Miscellaneous

Set Local Date (mm/dd)	Définit la date locale (où « mm » correspond aux mois et « dd » aux jours). L'année est facultative et peut être composée de deux ou quatre chiffres. **REMARQUE :** Il n'est généralement pas nécessaire de définir cette valeur pour la date des applications vocales et l'heure est synchronisée avec la SRP. Reportez-vous à la page **Administration > Time Setup**.
Set Local Time (HH/mm)	Définit l'heure locale (où « hh » correspond aux heures et « mm » aux minutes). Les secondes sont facultatives.
FXS Port Impedance	Définit l'impédance électrique du port FXS. Options disponibles : 600, 900, 600+2.16uF, 900+2.16uF, 270+750‖150nF, 220+850‖120nF, 220+820‖115nF, or 200+600‖100nF. La valeur par défaut est 600. **REMARQUE** Pour l'impédance de la Nouvelle Zelande (370+620‖310nF), utilisez 270+750‖150nF.
FXS Port Input Gain	Gain en entrée en décibels (dB), jusqu'à trois décimales. Ce nombre peut être compris entre 6,000 et 12,000. La valeur par défaut est -3.
FXS Port Output Gain	Gain en sortie en décibels (dB), jusqu'à trois décimales. Ce nombre peut être compris entre 6,000 et 12,000. Les tonalités de progression d'appel et le niveau de lecture DTMF ne sont pas affectés par le paramètre FXS Port Output Gain. La valeur par défaut est -3.
DTMF Playback Level	Niveau de lecture DTMF locale en décibels (dBm) jusqu'à une décimale. La valeur par défaut est -16.0.

DTMF Playback Twist	Différence de volume entre les fréquences de tonalité hautes et basses. La valeur par défaut est 1,3.
DTMF Playback Length	Durée de lecture DTMF locale en millisecondes. La valeur par défaut est.1.
Detect ABCD	Sélectionnez yes pour activer la détection locale de DTMF ABCD. Sinon, sélectionnez no. La valeur par défaut est yes. Ce paramètre n'a aucun effet si le paramètre DTMF Tx Method est configuré sur INFO ; ABCD est toujours envoyé hors bande quel que soit ce paramètre.
Playback ABCD	Sélectionnez yes pour activer la lecture locale deOOB DTMF ABCD. Sinon, sélectionnez no. La valeur par défaut est yes.

Caller ID Method	Les options suivantes sont : **Bellcore (N.Amer,China)** : CID, CIDCW et VMWI. FSK envoyé après la première sonnerie (identique à ETSI FSK envoyé après la première sonnerie) (sans inversion de la polarité ou DTAS). **DTMF (Finland, Sweden)** : CID uniquement. DTMF envoyé après l'inversion de la polarité (sans DTAS) et avant la première sonnerie. **DTMF (Denmark)** : CID uniquement. DTMF envoyé avant la première sonnerie sans inversion de polarité, ni DTAS. **ETSI DTMF :** CID uniquement. DTMF envoyé après DTAS (sans inversion de la polarité) et avant la première sonnerie. **ETSI DTMF With PR** : CID uniquement. DTMF envoyé après l'inversion de la polarité et DTAS et avant la première sonnerie. **ETSI DTMF After Ring** : CID uniquement. DTMF envoyé après la première sonnerie (sans inversion de la polarité ou DTAS). **ETSI FSK :** CID, CIDCW et VMWI. FSK envoyé après DTAS (sans inversion de la polarité) et avant la première sonnerie. En attente d'ACK de CPE après DTAS pour CIDCW. **ETSI FSK With PR (R.-U.)** : CID, CIDCW et VMWI. FSK est envoyé après l'inversion de la polarité et DTAS et avant la première sonnerie. En attente d'ACK de CPE après DTAS pour CIDCW. L'inversion de la polarité ne s'applique que si l'équipement est raccroché. La valeur par défaut est Bellcore(N.Amer, China).
FXS Port Power Limit	Les options sont comprises entre 1 et 8. La valeur par défaut est 3.
Caller ID FSK Standard	La SRP prend en charge les normes bell 202 et v.23 pour la génération de l'ID de l'appelant. La valeur par défaut est bell 202.
Feature Invocation Method	Sélectionnez la méthode que vous souhaitez utiliser : Default ou Sweden default. La valeur par défaut est Default.

Pages Line (1-4)

Utilisez les pages Line pour configurer les lignes pour des services vocaux.

REMARQUE Selon votre numéro de modèle, le nombre de lignes disponibles peut varier. Les modèles SRP520-U prennent en charge 2 lignes uniquement (Line 1 et Line 2), tandis que les modèles SRP540 prennent en charge 4 lignes (Line 1–4).

Ces pages incluent les sections suivantes :

- **Line Enable**
- **Streaming Audio Server**
- **Paramètres NAT**
- **Paramètres réseau**
- **Paramètres SIP**
- **Paramètres de la fonctionnalité d'appel**
- **Proxy et enregistrement**
- **Informations sur l'abonné**
- **Abonnement à un service supplémentaire**
- **Configuration audio**
- **Plan de numérotation**
- **Configuration de la polarité du port FXS**

Dans un profil de configuration, les paramètres Line doivent être ajoutés avec les chiffres appropriés (par exemple, [1] ou [2]) afin d'identifier la ligne à laquelle le paramètre s'applique.

Line Enable

Voice > Line 1–4 > Line Enable

Line Enable	Pour activer cette ligne, sélectionnez **yes**. Sinon, sélectionnez no. La valeur par défaut est yes.

Streaming Audio Server

Voice > Line 1–4 > Streaming Audio Server (SAS)

SAS Enable	Sélectionnez yes pour activer l'utilisation de cette ligne en tant que source de flux audio. Sinon, sélectionnez no. Si elle est activée, la ligne ne peut pas être utilisée pour les appels sortants. Elle est utilisée pour répondre automatiquement aux appels entrants et pour diffuser des paquets RTP audio vers l'appelant. La valeur par défaut est no.
SAS DLG Refresh Intvl	Si cette valeur est différente de zéro, il s'agit de l'intervalle avec lequel le serveur de flux audio envoie des messages d'actualisation de session (re-INVITE SIP) pour déterminer si la connexion de l'appelant est encore active. Si l'appelant ne répond pas au message d'actualisation, la SRP met fin à l'appel à l'aide d'un message SIP BYE. L'intervalle est compris entre 0 et 255 secondes (0 signifie que l'actualisation de session est désactivée). La valeur par défaut est 30.

SAS Inbound RTP Sink	Ce paramètre s'applique aux périphériques qui ne lisent pas le RTP entrant si la ligne du serveur de flux audio se déclare elle-même comme un périphérique d'envoi uniquement et demande au client de ne pas diffuser de données audio. Saisissez le nom de domaine complet (FQDN) ou l'adresse IP du bloc récepteur RTP ; cette valeur est utilisée par la ligne du serveur de flux audio dans le SDP de sa réponse 200 à un message INVITE entrant provenant d'un client. L'objectif de ce paramètre est de fonctionner avec des périphériques qui ne lisent pas les RTP entrants si la ligne SAS se déclare comme périphérique en envoi seul et indique au client de ne pas transmettre de données audio. Ce paramètre est un FQDN ou l'adresse IP du bloc récepteur RTP à utiliser par la ligne SAS du SDP pour la réponse 200 au message INVITE entrant émanant d'un client. Il apparaît dans c = ligne et le numéro de port et, s'il est spécifié, dans m = ligne du SDP. Si cette valeur n'est pas spécifiée ou si elle est égale à 0, c = 0.0.0.0 et a=sendonly est utilisé dans le SDP pour indiquer au client SAS de ne pas envoyer de RTP à cette ligne SAS. Si une valeur autre que zéro est spécifiée, a=sendrecv et le client SAS transmet en continu les données audio à l'adresse indiquée. Cas particulier : si la valeur est égale à $IP, l'adresse IP de la ligne SAS est utilisée dans c = line et a = sendrecv. Dans ce cas, le client SAS transmet en continu des paquets RTP à la ligne SAS. Aucune valeur par défaut n'est définie.

Paramètres NAT

Voice > Line 1–4 > NAT Settings

NAT Mapping Enable	Utilisé pour mapper en externe des adresses IP et les ports de SIP/RTP dans les messages SIP. La valeur par défaut est no. **REMARQUE** En général, vous n'aurez pas besoin de modifier ce paramètre, car les ports vocaux sont rattachés à l'interface WAN (et ne sont pas donc soumis au NAT).
NAT Keep Alive Enable	Pour envoyer périodiquement le message de maintien de connexion NAT configuré, sélectionnez yes. Sinon, sélectionnez no. La valeur par défaut est no.
NAT Keep Alive Msg	Saisissez le message de maintien de connexion devant être envoyé périodiquement afin de maintenir le mappage NAT actuel. Si cette valeur est $NOTIFY, un message NOTIFY est envoyé. Si cette valeur est $REGISTER, un message REGISTER sans contact est envoyé. La valeur par défaut est $NOTIFY.
NAT Keep Alive Dest	Destination des messages de maintien de connexion NAT. Si la valeur est $PROXY, les messages sont envoyés au serveur proxy actuel ou au serveur proxy sortant. La valeur par défaut est $PROXY.

Paramètres réseau

Voice > Line 1–4 > Network Settings

SIP ToS/DiffServ Value	Valeur du champ TOS/DiffServ dans les paquets IP UDP transportant un message SIP. La valeur par défaut est 0x68.
SIP CoS Value [0-7]	Valeur CoS des messages SIP. La valeur par défaut est 3.

RTP ToS/DiffServ Value	Valeur du champ ToS/DiffServ dans les paquets IP UDP transportant des données RTP. La valeur par défaut est 0xb8**.**
RTP CoS Value [0- 7]	Valeur CoS des données RTP. La valeur par défaut est 6**.**
Network Jitter Level	Permet de déterminer la manière dont la taille du tampon d'instabilité est ajustée par la SRP. Elle est ajustée de manière dynamique. Pour tous les paramètres de niveau d'instabilité, la taille minimale du tampon d'instabilité est de 30 millisecondes ou de (10 millisecondes + la taille de la trame RTP actuelle), la taille la plus élevée étant privilégiée. Néanmoins, la valeur de la taille du tampon d'instabilité de début est plus élevée pour des niveaux d'instabilité supérieurs. Ce paramètre contrôle le taux d'ajustement de la taille du tampon d'instabilité pour que cette dernière soit la moins élevée possible. Sélectionnez le paramètre approprié : **low**, **medium**, **high**, **very high**, or **extremely high**. La valeur par défaut est high.
Jitter Buffer Adjustment	Permet de déterminer la manière dont le tampon d'instabilité doit être ajusté. Sélectionnez le paramètre approprié : **up and down**, **up only**, **down only**, or **disable**. Le paramètre par défaut est up and down.
Auto PSTN Fallback	Pour permettre au routeur de la ligne d'appeler le port FXO lorsque le service IP n'est pas disponible, sélectionnez **yes**. Sinon, sélectionnez **no**. La valeur par défaut est yes.

Paramètres SIP

Voice > Line 1–4 > SIP Settings

SIP Transport	Le protocole TCP offre une « remise garantie » qui assure la retransmission des paquets perdus. Le TCP garantit aussi la réception des paquets SIP dans le même ordre que leur envoi. Par conséquent, le TCP surmonte les principaux inconvénients du protocole UDP. Par ailleurs, pour des raisons de sécurité, la plupart des pare-feux d'entreprise bloquent les ports UDP. Avec le TCP, l'ouverture des nouveaux ports ou l'abandon des paquets n'est pas obligatoire. Le TCP fonctionne déjà pour les activités de base comme la recherche Internet ou le commerce en ligne. Les options sont les suivantes : **UDP**, **TCP**, **TLS**. La valeur par défaut est UDP.
SIP Port	Numéro du port d'écoute et de transmission des messages SIP. La valeur par défaut est 5060.
SIP 100REL Enable	Pour activer la prise en charge de l'extension SIP 100REL afin de garantir la fiabilité de transmission des réponses provisoires (18x) et l'utilisation les demandes PRACK, sélectionnez **yes**. Sinon, sélectionnez **no**. La valeur par défaut est no.
EXT SIP Port	Numéro de port SIP externe.
Auth Resync-Reboot	Si cette fonctionnalité est activée, la SRP authentifie l'expéditeur lorsqu'il reçoit un message NOTIFY resync reboot (RFC 2617). Pour activer cette fonctionnalité, sélectionnez **yes**. Sinon, sélectionnez **no**. La valeur par défaut est yes.

SIP Proxy-Require	Le proxy SIP peut prendre en charge un poste ou un comportement spécifique lorsqu'il détecte cet en-tête chez l'agent utilisateur. Si ce champ est configuré et que le proxy ne le prend pas en charge, il envoie un message de non prise en charge. Saisissez l'en-tête approprié dans le champ approprié.
SIP Remote-Party-ID	Sélectionnez **yes** pour utiliser l'en-tête Remote-Party-ID plutôt que l'en-tête From. Sinon, sélectionnez **no**. La valeur par défaut est yes.
SIP GUID	L'identifiant global unique est généré pour chaque ligne de chaque périphérique. Lorsqu'il est activé, la SRP ajoute un en-tête GUID à la requête SIP. Le GUID est généré au premier démarrage de l'unité et demeure sur l'unité lors des redémarrages ultérieurs et également lors du rétablissement des paramètres d'usine. Cette fonctionnalité a été demandée par Bell Canada (Nortel) afin de limiter les enregistrements de comptes SIP. La valeur par défaut est no.

SIP Debug Option	Les messages SIP sont reçus depuis ou envoyés vers le port d'écoute du proxy. Cette fonctionnalité permet de contrôler les messages SIP à consigner. Vous pouvez choisir l'une des options suivantes : ▪ **none** : aucune consignation. ▪ **1-line** : consigne uniquement la première ligne de tous les messages. ▪ **1-line excl. OPT** : consigne uniquement la première ligne de tous les messages hormis les requêtes/réponses OPTIONS. ▪ **1-line excl. NTFY** : consigne uniquement la première ligne de tous les messages hormis les requêtes/réponses NOTIFY. ▪ 1**-line excl. REG** : consigne uniquement la première ligne de tous les messages hormis les requêtes/réponses REGISTER. ▪ **1-line excl. OPTINTFYIREG** : consigne uniquement la première ligne de tous les messages hormis les requêtes/réponses OPTIONS, NOTIFY et REGISTER. ▪ **full** : consigne le texte intégral de tous les messages SIP. ▪ **full excl. OPT** : consigne le texte intégral de tous les messages SIP hormis les requêtes/réponses OPTIONS. ▪ **full excl. NTFY** : consigne le texte intégral de tous les messages SIP hormis les requêtes/réponses NOTIFY. ▪ **full excl. REG** : consigne le texte intégral de tous les messages SIP hormis les requêtes/réponses REGISTER. ▪ **full excl. OPTINTFYIREG** : consigne le texte intégral de tous les messages SIP hormis les requêtes/réponses OPTIONS, NOTIFY et REGISTER. La configuration par défaut est none.

RTP Log Intvl	Intervalle du journal RTP. La valeur par défaut est 0.
Restrict Source IP	Si les lignes 1 et 2 utilisent la même valeur de port SIP et que la fonction Restrict Source IP est activée, l'adresse IP du proxy des lignes 1 et 2 est considérée comme une adresse IP acceptable pour ces deux lignes. Pour activer la fonction Restrict Source IP, sélectionnez yes. Sinon, sélectionnez no. Si elle est configurée, la SRP déposera tous les paquets envoyés à ses ports SIP en provenance d'une adresse IP non approuvée. Une adresse IP source n'est pas fiable si elle ne correspond pas à l'une des adresses IP résolues par le Proxy configuré (ou Outbound Proxy si Use Outbound Proxy est activé). La valeur par défaut est no.
Referor Bye Delay	Permet de déterminer le moment où la SRP envoie un message BYE pour arrêter les branches d'appel en attente à la fin des transferts d'appel. Plusieurs paramètres de délai sont configurés sur cet écran : Referor, Refer Target, Referee et Refer-To Target. Pour le paramètre Referor Bye Delay, saisissez le délai adéquat en secondes. La valeur par défaut est 4.
Refer Target Bye Delay	Pour le paramètre Refer Target Bye Delay, saisissez le délai adéquat en secondes. La valeur par défaut est 0.
Referee Bye Delay	Pour le paramètre Referee Bye Delay, saisissez le délai adéquat en secondes. La valeur par défaut est 0.
Refer-To Target Contact	Pour contacter Refer-To Target, sélectionnez yes. Sinon, sélectionnez no. La valeur par défaut est no.

Sticky 183	Si cette fonctionnalité est activée, la SRP ignore toutes les réponses SIP 180 postérieures à la réception de la première réponse SIP 183 à un message INVITE sortant. Pour activer cette fonction, sélectionnez yes. Sinon, sélectionnez no. La valeur par défaut est no.
Use Anonymous With RPID	Lorsque la fonctionnalité est définie sur yes, utilisez « anonymous » dans le message SIP. La valeur par défaut est yes.
Use Local Addr In From	Utilisez l'adresse IP locale de la SRP dans le message FROM du SIP. La valeur par défaut est no.
Auth INVITE	Si ce paramètre est activé, une autorisation est nécessaire pour les requêtes initiales INVITE entrantes du proxy SIP.
Reply 182 On Call Waiting	Lorsque la fonctionnalité est activée, la SRP répond avec une réponse SIP 182 à l'appelant s'il est déjà en communication et si la ligne est décrochée. Pour utiliser cette fonctionnalité, sélectionnez **yes**. La valeur par défaut est no.

Paramètres de la fonctionnalité d'appel

Voice > Line 1–4 > Call Feature Settings

Blind Attn-Xfer Enable	Permet à la SRP d'effectuer une opération de renvoi manuel d'appel en mettant fin à la branche d'appel en cours et en procédant à un transfert aveugle de l'autre branche d'appel. Si cette fonctionnalité est désactivée, la SRP effectue une opération de transfert d'appel en renvoyant l'autre branche d'appel vers la branche d'appel actuelle tout en maintenant les deux. Pour activer cette fonctionnalité, sélectionnez **yes**. Sinon, sélectionnez **no**. La valeur par défaut est no.

MOH Server	ID utilisateur ou URL du serveur de flux audio de la réponse automatique. Lorsqu'un seul ID utilisateur est spécifié, le proxy actuel ou sortant est contacté. Si le serveur MOH n'est pas spécifié, la musique d'attente est désactivée.
Xfer When Hangup Conf	Le périphérique SRP effectue un transfert à la fin de la conférence téléphonique. Sélectionnez **yes** ou **no** dans le menu déroulant. La valeur par défaut est yes.
Conference Bridge URL	Cette fonctionnalité permet de prendre en charge l'interconnexion de conférence externe pour les conférences téléphoniques à n participants (n>2), plutôt que de mixer le flux audio en local. Pour utiliser cette fonctionnalité, définissez ce paramètre sur celui du nom de serveur. Par exemple : conf@mysefver.com:12345 ou conf (qui utilise la valeur du proxy comme domaine).
Conference Bridge Ports	Permet de sélectionner le nombre maximal de participants à une conférence téléphonique. Ce nombre peut être compris entre 3 et 10. La valeur par défaut est 3.

Proxy et enregistrement

Voice > Line 1–4 > Proxy and Registration

Proxy	Serveur proxy SIP pour toutes les requêtes sortantes.
Outbound Proxy SIP	Serveur proxy SIP sortant vers lequel toutes les demandes sortantes sont envoyées comme premier saut.
Use Outbound Proxy	Permet l'utilisation d'un proxy sortant. Si no est sélectionné, les paramètres Outbound Proxy et Use OB Proxy in Dialog sont ignorés. La valeur par défaut est no.

Use OB Proxy In Dialog	Permet de forcer l'envoi des requêtes SIP vers le proxy sortant dans une boîte de dialogue. Ignoré si le paramètre Use Outbound Proxy n'est pas sélectionné ou si le paramètre Outbound Proxy est vide. La valeur par défaut est yes.
S'inscrire	Permet d'activer l'enregistrement périodique à l'aide du paramètre Proxy. Ce paramètre est ignoré si Proxy n'est pas indiqué. La valeur par défaut est yes.
Make Call Without Reg	Permet d'effectuer des appels sortants sans enregistrement réussi (dynamique) de l'unité. Dans le cas contraire, aucune tonalité n'est émise sauf en cas de confirmation de l'enregistrement. La valeur par défaut est no.
Register Expires	Valeur d'expiration en secondes dans une requête REGISTER. Le SRP renouvelle périodiquement l'enregistrement un peu avant l'expiration de l'enregistrement. Ce paramètre est ignoré si le paramètre Register est no. Plage : 0 – (2^{31} – 1) sec. La valeur par défaut est 3600.
Ans Call Without Reg	Permet de répondre à des appels entrants sans enregistrement réussi (dynamique) de l'unité. La valeur par défaut est no.
Use DNS SRV	Permet d'indiquer si la recherche DNS SRV est utilisée pour le proxy et le proxy sortant. La valeur par défaut est no.
DNS SRV Auto Prefix	S'il est activé, le SRP ajoute automatiquement le préfixe _sip._udp au nom Proxy ou Outbound Proxy lorsqu'une recherche DNS SRV est effectuée sur ce nom. La valeur par défaut est no.

Proxy Fallback Intvl	Ce paramètre définit le délai, en secondes, après lequel le SRP fait une nouvelle tentative depuis les serveurs proxy (ou proxy sortant) ayant la priorité la plus élevée après avoir échoué avec un serveur de priorité inférieure. Ce paramètre fonctionne uniquement si la liste de serveurs proxy principal et de sauvegarde a été fournie au SRP via la recherche d'enregistrement du serveur DNS SRV sur le nom de serveur. (L'utilisation d'un enregistrement DNS A multiple par nom de serveur n'autorise pas la notion de priorité. Tous les hôtes sont alors considérés selon le même niveau de priorité et le SRP n'essaye pas de revenir en arrière après un échec). La valeur par défaut est 3600.
Proxy Redundancy Method	Sélectionnez le port Normal ou Based on SRV. La SRP crée une liste interne des proxys renvoyés dans les enregistrements DNS SRV. Si vous sélectionnez Normal, la liste contient des proxies classés par poids et priorité. Si vous sélectionnez Based on SRV Port, la SRP utilise la fonctionnalité Normal, puis inspecte le numéro de port en s'appuyant sur le premier port de proxy de la liste. La valeur par défaut est Normal.
Voice Mail Server	Permet de saisir l'URL ou l'adresse IP du serveur.
Mailbox Subscribe Expires	Définit l'intervalle d'abonnement pour l'indication de message vocal en attente.

Informations sur l'abonné

Voice > Line 1–4 > Informations sur l'abonné

Display Name	Nom d'affichage de l'ID de l'appelant.
User ID	ID utilisateur pour cette ligne.
Password	Mot de passe de cette ligne.

Use Auth ID	Pour utiliser l'ID et le mot de passe de l'authentification SIP, sélectionnez yes. Sinon, sélectionnez no pour utiliser l'ID et le mot de passe utilisateur. La valeur par défaut est no.
Auth ID	ID d'authentification SIP.
Directory Number	Saisissez le numéro de cette ligne.
Mini Certificate	Mini certificat (codé Base64) concaténé avec la clé publique 1024 bits du CAavec comme signature le MC de tous les abonnés du groupe. Aucune valeur par défaut n'est définie.
SRTP Private Key	Clé privée par abonné de 512 bits, codée base64 pour l'établissement d'un appel sécurisé. Aucune valeur par défaut n'est définie.

Abonnement à un service supplémentaire

La SRP offre une prise en charge native de nombreux services avancés ou supplémentaires. Tous ces services sont facultatifs. Les paramètres figurant dans le tableau ci-dessous permettent d'activer ou de désactiver un service supplémentaire spécifique. Un service supplémentaire doit être désactivé si a) l'utilisateur n'y a pas souscrit ou b) le fournisseur d'accès prend en charge un service similaire en utilisant un autre équipement que la SRP.

Voice > Line 1–4 > Supplementary Service Subscription

Call Waiting Serv	Permet d'activer le service d'appel en attente. La valeur par défaut est yes.
Block CID Serv	Permet d'activer le service de blocage de l'ID de l'appelant. La valeur par défaut est yes.
Block ANC Serv	Permet d'activer le service de blocage des appels anonymes. La valeur par défaut est yes.
Dist Ring Serv	Permet d'activer le service de sonnerie distincte. La valeur par défaut est yes.

Cfwd All Serv	Permet d'activer le service de transfert de tous les appels. La valeur par défaut est yes.
Cfwd Busy Serv	Permet d'activer le service de transfert d'appel si occupé. La valeur par défaut est yes.
Cfwd No Ans Serv	Permet d'activer le service de transfert d'appel si pas de réponse. La valeur par défaut est yes.
Cfwd Sel Serv	Permet d'activer le service de transfert d'appel sélectif. La valeur par défaut est yes.
Cfwd Last Serv	Permet d'activer le service de transfert du dernier appel. La valeur par défaut est yes.
Block Last Serv	Permet d'activer le service de blocage du dernier appel. La valeur par défaut est yes.
Accept Last Serv	Permet d'activer le service d'acceptation du dernier appel La valeur par défaut est yes.
DND Serv	Permet d'activer le service Ne pas déranger La valeur par défaut est yes.
CID–Serv	Permet d'activer le service d'identification de l'appelant La valeur par défaut est yes.
CWCID Serv	Permet d'activer le service de mise en attente de l'ID de l'appelant. La valeur par défaut est yes.
Call Return Serv	Permet d'activer le service de renvoi d'appel La valeur par défaut est yes.
Call Redial Serv	Permet d'activer le service de recomposition de l'appel.

Call Back Serv	Permet d'activer le service de rappel.
Three Way Call Serv	Permet d'activer le service d'appel à trois parties. L'appel à trois parties est nécessaire pour les conférences à trois participants et pour le transfert supervisé. La valeur par défaut est yes.
Three Way Conf Serv	Permet d'activer le service de conférence à trois participants. La conférence à trois participants est nécessaire pour le transfert supervisé. La valeur par défaut est yes.
Attn Transfer Serv	Permet d'activer le service de transfert d'appel supervisé. La conférence à trois participants est nécessaire pour le transfert supervisé. La valeur par défaut est yes.
Unattn Transfer Serv	Permet d'activer le service de renvoi d'appel non surveillé (transfert en aveugle). La valeur par défaut est yes.
MWI Serv	Permet d'activer le service MWI. Le service MWIest disponible uniquement si un service de messagerie vocale est configuré dans le déploiement. La valeur par défaut est yes.
VMWI Serv	Permet d'activer le service VMWI (FSK). La valeur par défaut est yes.
Speed Dial Serv	Permet d'activer le service de numérotation rapide. La valeur par défaut est yes.
Secure Call Serv	Permet d'activer le service d'appel sécurisé. La valeur par défaut est yes.
Referral Serv	Permet d'activer le service de référence. Pour plus de détails, reportez-vous au paramètre Referral Services Codes. La valeur par défaut est yes.

Feature Dial Serv	Permet d'activer le service de la fonctionnalité de numérotation Pour plus de détails, reportez-vous au paramètre Feature Dial Services Codes. La valeur par défaut est yes.
Service Announcement Serv	Permet d'activer le service d'annonce. La valeur par défaut est yes.

Configuration audio

Voice > Line 1–4 > Audio Configuration

Preferred Codec	Codec préféré pour tous les appels. (Le codec réel utilisé dans un appel dépend toujours des résultats du protocole de négociation du codec.) Sélectionnez l'une des options suivantes : **G711u, G711a, G726-32** ou **G729a.** La valeur par défaut est G711u.
Second Preferred Codec	Deuxième codec préféré pour tous les appels. (Le codec réel utilisé dans un appel dépend toujours des résultats du protocole de négociation du codec.) Sélectionnez un des éléments suivants : **Unspecified**, **G711u, G711a, G726-32** ou **G729a.** La valeur par défaut est Unspecified.
Third Preferred Codec	Troisième codec préféré pour tous les appels. (Le codec réel utilisé dans un appel dépend toujours des résultats du protocole de négociation du codec.) Sélectionnez l'une des options suivantes : **Unspecified, G711u, G711a, G726-16, G726-24, G726-32, G726-40, G729a** ou **G723.** La valeur par défaut est Unspecified.
Use Pref Codec Only	Pour utiliser uniquement le codec de votre choix pour tous les appels, sélectionnez **yes**. (L'appel échoue si l'extrémité ne prend pas en charge ce codec.) Sinon, sélectionnez **no**. La valeur par défaut est no.

Silence Supp Enable	Pour activer la suppression des silences de manière à ce que les trames audio silencieuses ne soient pas transmises, sélectionnez **yes**. Sinon, sélectionnez **no**. La valeur par défaut est no.
Silence Threshold	Sélectionnez le paramètre approprié pour le seuil : high, medium ou low. Le niveau moyen est défini par défaut.
G729a enable	Pour activer l'utilisation du codec G.729a à 8 Kbit/s, sélectionnez yes. Sinon, sélectionnez **no**. La valeur par défaut est yes.
Echo Canc Enable	Pour activer l'utilisation de l'annuleur d'écho, sélectionnez **yes**. Sinon, sélectionnez **no**. La valeur par défaut est yes.
Echo Canc Adapt Enable	Pour activer l'adaptation du suppresseur d'écho, sélectionnez **yes**. Sinon, sélectionnez **no**. La valeur par défaut est yes.
Echo Supp Enable	Pour activer l'utilisation du suppresseur d'écho, sélectionnez **yes**. Sinon, sélectionnez **no**. La valeur par défaut est yes.
Echo Cancel Delay	Pour activer l'utilisation du délai d'annulation d'écho, sélectionnez **yes**. Sinon, sélectionnez **no**. La valeur par défaut est yes.
Echo Cancel Tail	Pour activer l'utilisation de la mise en file d'attente de suppression d'écho, sélectionnez **yes**. Sinon, sélectionnez **no**. La valeur par défaut est yes.
FAX V21 Detect Enable	Pour activer la détection des tonalités du télécopieur V21, sélectionnez **yes**. Sinon, sélectionnez **no**. La valeur par défaut est yes.
G726-32 enable	Pour activer l'utilisation du codec G.726 à 32 Kbits/s, sélectionnez **yes**. Sinon, sélectionnez **no**. La valeur par défaut est yes.

FAX CNG Detect Enable	Pour activer la détection de la tonalité d'appel du télécopieur (CNG), sélectionnez **yes**. Sinon, sélectionnez **no**. La valeur par défaut est yes.
FAX Passthru Codec	Sélectionnez le codec de diffusion de télécopie G711u ou G711a. La valeur par défaut est G711u.
DTMF Process INFO	Pour utiliser la fonction d'information lors du traitement DTMF, sélectionnez yes. Sinon, sélectionnez **no**. La valeur par défaut est yes.
FAX Codec Symmetric	Pour forcer la SRP à utiliser un codec symétrique en mode télécopie permettant le trafic via un port voix, sélectionnez **yes**. Sinon, sélectionnez **no**. La valeur par défaut est yes.
DTMF Process AVT	Pour utiliser la fonctionnalité AVT lors du processus DTMF, sélectionnez **yes**. Sinon, sélectionnez **no**. La valeur par défaut est yes.
FAX Passthru Method	Sélectionnez la méthode télécopie permettant le trafic via un port voix : None, NSE ou ReINVITE. La valeur par défaut est NSE.
DTMF Tx Method	Sélectionnez la méthode de transmission des signaux DTMF à l'extrémité : **InBand, AVT, INFO** ou **Auto**. La méthode InBand envoie les signaux DTMF à l'aide du chemin audio. La méthode AVT envoie les signaux DTMF en tant qu'événements AVT. La méthode INFO utilise la méthode SIP INFO. La méthode Auto utilise la méthode InBand ou AVT, basée sur les résultats de la négociation de codecs. La méthode par défaut est Auto.

DTMF Tx Mode	Le **mode Tx de détection DTMF** est disponible pour les informations SIP et AVT. Les options sont les suivantes : **Strict** ou **Normal**. La valeur par défaut est Strict pour laquelle les conditions suivantes sont remplies : Les **chiffres DTMF** ont besoin d'un temps d'attente supplémentaire après la détection. Le seuil du **niveau DTMF** est augmenté à -20 dBm. Les seuils de durée minimaux et maximaux sont : ▪ mode strict pour AVT : 70 ms ▪ mode normal pour AVT : 40 ms ▪ mode strict pour les informations SIP : 90 ms ▪ mode normal pour les informations SIP : 50 ms
FAX Process NSE	Pour utiliser la fonctionnalité NSE lors du processus de télécopie, sélectionnez **yes**. Sinon, sélectionnez **no**. La valeur par défaut est yes.
Hook Flash Tx Method	Sélectionnez la méthode de signalement des événements d'actionnement du crochet commutateur : None, AVT ou INFO. La méthode None ne signale pas les événements de crochet commutateur. La méthode AVT utilise le RFC2833 AVT (événement = 16). La méthode INFO utilise le SIP INFO et inclut uniquement la ligne signal=hf dans le corps du message. Le type MIME du corps de ce message provient du paramètre du crochet commutateur, type MIME. La valeur par défaut est Aucun.
FAX Disable ECAN	Si elle est activée, cette fonction désactive automatiquement le correcteur d'écho lorsqu'une tonalité de fax est détectée. Pour activer cette fonctionnalité, sélectionnez **yes**. Sinon, sélectionnez **no**. La valeur par défaut est no**.**

Release Unused Codec	Cette fonction permet de libérer les codecs non utilisés après la négociation de codecs sur le premier appel afin que d'autres codecs puissent être utilisés pour la deuxième ligne. Pour activer cette fonctionnalité, sélectionnez **yes**. Sinon, sélectionnez **no**. La valeur par défaut est yes.
FAX Enable T38	Pour activer l'utilisation de la norme ITU-T T.38 pour FAX Relay, sélectionnez **yes**. Sinon, sélectionnez **no**. La valeur par défaut est yes.
FAX T38 Redundancy	Sélectionnez le nombre approprié pour indiquer le nombre de charges utiles de paquet précédentes à la répétition avec chaque paquet. Sélectionnez 0 pour aucune redondance de la charge utile. Plus le nombre est élevé, plus la taille des paquets et la bande passante consommée sont importantes. La valeur par défaut est 1.
FAX T38 ECM Enable	Sélectionnez **yes** pour activer le mode T.38 de correction des erreurs. Sinon, sélectionnez **no**.
Fax Tone Detect Mode	Ce paramètre comporte trois valeurs possibles : **caller or callee** : la SRP détecte la tonalité de fax qu'il s'agisse de l'appelant ou de l'appelé. **caller only :** la SRP détecte la tonalité de fax uniquement s'il s'agit de l'appelant. **callee only** : la SRP détecte la tonalité de fax uniquement s'il s'agit de l'appelé. La valeur par défaut est caller or callee.
Auto Dump Option1/ Option2	Paramètres utilisés par l'assistance clientèle pour capturer l'audio sur la ligne.

Plan de numérotation

Le script du plan de numérotation par défaut pour chaque ligne est le suivant : (*xx|[3469]11|0|00|[2- 9]xxxxxx|1xxx[2-9]xxxxxx|xxxxxxxxxxx.). La syntaxe d'une expression du plan de numérotation est décrite dans le tableau ci-dessous.

Voice > Line 1–4 > Dial Plan

Entrée du plan de numérotation	Fonctionnalité
*xx	Autorise un code étoile à deux chiffres
[3469]11	Autorise des séquences x11
0	Opérateur
00	Opérateur international
[2-9]xxxxxxxx	Numéro local des États-Unis
1xxx[2-9]xxxxxx	Numéro longue distance avec 10 chiffres + 1 pour les États-Unis
xxxxxxxxxxx.	Tout le reste (longue distance internationale, FWD, ...)

Dial Plan	Script du plan de numérotation pour cette ligne. La valeur par défaut est (*xx|[3469]11|0|00|[2-9]xxxxxx|1xxx[2- 9]xxxxxxS0|xxxxxxxxxxx.) Chaque paramètre est séparé par un point-virgule (;). Exemple 1 : *1xxxxxxxxxx<:@fwdnat.pulver.com:5082;uid=jsmith;pwd=xy z Exemple 2 : *1xxxxxxxxxx<:@fwd.pulver.com;nat;uid=jsmith;pwd=xyz Exemple 3 : [39]11<:@gw0>
PSTN Fallback Dial Plan	Script du plan de numérotation pour acheminer des appels vers le port FXO lorsque le service IP n'est pas disponible. Le script par défaut est (S0<:@gw0>).

Enable IP Dialing	Permet d'activer ou de désactiver la numérotation IP. Si la numérotation IP est activée, il faut composer [user-id@]a.b.c.d[:port], où « @ », « . » et « : » sont composés en saisissant le caractère * ; l'ID utilisateur doit être composé de caractères numériques (comme un numéro de téléphone) ; a, b, c et d doivent être compris entre 0 et 255 ; et le port doit être supérieur à 255. Si le port n'est pas donné, 5060 est utilisé. Le port et l'ID utilisateur sont facultatifs. Si l'ID utilisateur correspond à un modèle du plan de numérotation, il est alors interprété comme un numéro de téléphone normal selon le plan de numérotation. Cependant, le message INVITE est toujours envoyé au proxy sortant s'il est activé. La valeur par défaut est no.
Emergency Number	Liste de modèles de numéros d'urgence séparés par des virgules. Si l'appel sortant correspond à l'un de ces modèles, la SRP désactive le traitement de l'événement d'actionnement du crochet commutateur. La condition est restaurée à la normale lorsque l'appel se termine. Un espace vide indique l'absence de numéro d'urgence. 63 caractères au maximum. Par défaut, cette valeur n'est pas définie.

Configuration de la polarité du port FXS

Voice > Line 1–4 > FXS Port Polarity Configuration

Idle Polarity	La polarité avant un appel est connectée : Forward ou Reverse. La valeur par défaut est Forward.
Caller Conn Polarity	La polarité après un appel sortant est connectée : Forward ou Reverse. La valeur par défaut est Forward.
Callee Conn Polarity	La polarité après un appel entrant est connectée : Forward ou Reverse. La valeur par défaut est Forward.

Page PSTN (modèles SRP540 uniquement)

Utilisez les pages PSTN pour configurer la ligne PSTN (Public Switched Telephone Network, Réseau téléphonique public commuté) sur la SRP.

Ces pages incluent les sections suivantes :

- **Activation de ligne PSTN**
- **Paramètres SIP**
- **Paramètres de sonnerie**
- **Valeurs du minuteur PSTN**
- **Détection de la déconnexion PSTN**
- **Paramètres internationaux**

Activation de ligne PSTN

Voice > PSTN > PSTN Line Enable

PSTN Line Enable	Pour activer cette ligne, sélectionnez yes. Sinon, sélectionnez no. La valeur par défaut est yes.
PSTN Contact List	Répertorier les ports téléphoniques qui doivent être informés des appels entrants. Répertorier les numéros de port requis séparés par « + ». Le paramètre par défaut informe tous les ports à l'aide de la liste 1+2+3+4.

Paramètres SIP

Voice > PSTN > SIP Settings

SIP Debug Option	Les messages SIP sont reçus depuis ou envoyés vers le port d'écoute du proxy. Cette fonctionnalité permet de contrôler les messages SIP à consigner. Les choix suivants sont disponibles : **none** : aucune consignation. **1-line** : consigne uniquement la première ligne de tous les messages. **full** : consigne le texte intégral de tous les messages SIP. La configuration par défaut est none.

Paramètres de sonnerie

Voice > PSTN > Ring Settings

Default Ring	Définit la sonnerie par défaut pour les appels émis depuis le PSTN. Sélectionnez 1-8 ou suivez les configurations propres à la ligne.

Valeurs du minuteur PSTN

Voice > PSTN > PSTN Timer Values (sec)

PSTN Ring Thru Delay	Délai en secondes avant le début de la sonnerie pour la ligne 1 après le début de la sonnerie PSTN. Afin que la ligne 1 puisse disposer des informations d'identification de l'appelant, le délai doit être supérieur au délai nécessaire pour effectuer la présentation de l'ID de l'appelant RTCP (par exemple, 5 s). La plage va de 0 à 255. La valeur par défaut est 1.
xPSTN Dialing Delay	Délai après le décrochage et avant que la SRP compose un numéro PSTN. La plage va de 0 à 255. La valeur par défaut est 1.
PSTN Ring Timeout	Délai après le déclenchement de la sonnerie et avant que la SRPne décide que la sonnerie PSTN a cessé. La plage va de 0 à 255. La valeur par défaut est 5.

PSTN Dial Digit Len	Permet de déterminer la durée de fonctionnement et d'arrêt de la transmission des chiffres via le port FXO. La syntaxe est on-time/off-time, où on-time et off-time sont exprimés en secondes à deux décimales, selon la plage comprise entre 0,05 et 3,00. La valeur par défaut est .2/.2. Si cette valeur n'est pas indiquée, la valeur par défaut est utilisée.
PSTN Hook Flash Len	Longueur du signal crochet commutateur en secondes. Lors d'un appel de la passerelle PSTN-to-VoIP, la SRP traite le signal hors bande du crochet commutateur envoyé par l'homologue VoIP via un crochet commutateur (signal de raccrochage momentané) sur le port FXO. Cette fonctionnalité permet à l'homologue VoIP de démarrer une conférence à trois participants et de transférer les appels suivants. La durée du signal de raccrochage peut être configurée à l'aide de ce paramètre. La valeur par défaut est 0.25. La plage est comprise entre 0,02 et 1,6 seconde.
PSTN Ring Thru CWT Delay	Permet d'indiquer le délai avant que les appels PSTN entrants fassent sonner la ligne 1 en utilisant une tonalité d'attente. La valeur par défaut est 3.

Détection de la déconnexion PSTN

Voice > PSTN > PSTN Disconnect Detection

Detect CPC	Le CPC correspond à un bref arrêt de la tension des fils de pointe et de nuque. Si cette fonction est activée, la SRP déconnecte les deux connexions d'appel lorsque ce signal est détecté. La valeur par défaut est yes.
Detect Polarity Reversal	Si cette fonctionnalité est activée, lorsque ce signal est détecté pendant un appel de la passerelle, le SPA déconnecte les deux branches d'appel. S'il s'agit d'un appel de la passerelle RTPC, la première inversion de polarité est ignorée et la 2nde déclenche la déconnexion. Pour un appel de la passerelle VoIP, la 1ère inversion de polarité déclenche la déconnexion. La valeur par défaut est yes.

Detect PSTN Long Silence	Si cette fonctionnalité est activée, la SRP déconnecte les deux branches d'appel de la passerelle lorsque la branche PSTN n'a plus d'activité vocale pendant une durée supérieure à celle spécifiée dans le paramètre PSTN Long Silence Duration pendant un appel de la passerelle. La valeur par défaut est no.
Detect VoIP Long Silence	Si cette fonctionnalité est activée, la SRP déconnecte les deux branches d'appel de la passerelle lorsque la branche VoIP n'a plus d'activité vocale pendant une durée supérieure au paramètre VoIPn Long Silence Duration pendant un appel de la passerelle. La valeur par défaut est no.
PSTN Long Silence Duration	Cette valeur correspond à la longueur minimale de silence (ou d'inactivité) du RTPC pour déclencher la déconnexion de l'appel de la passerelle, uniquement si le paramètre Detect PSTN Long Silence est activé. La valeur par défaut est 30.
VoIP Long Silence Duration	Cette valeur correspond à la longueur minimale de silence (ou d'inactivité) du VoIP pour déclencher la déconnexion de l'appel de la passerelle, iniquement si le paramètre Detect VoIP Long Silence est activé. La valeur par défaut est 30.
PSTN Silence Threshold	Ce paramètre permet d'ajuster la sensibilité de la détection du silence RTPC. Choisissez entre {very low, low, medium, high, very high}. Plus ce paramètre est élevé, plus il est facile de détecter un silence et donc de déclencher une déconnexion. Le niveau moyen est défini par défaut.
Min CPC Duration	Permet de déterminer la durée minimale de basse tension des fils de pointe et de nuque (inférieure à 1 V) pour que la passerelle la reconnaisse comme un signal CPC ou un retrait de ligne RTPC. La valeur par défaut est 0.2.
Detect Disconnect Tone	Si ce paramètre est activé, la SRP déconnecte les deux branches d'appel de la passerelle lorsqu'il détecte la tonalité de déconnexion de la branche PSTN pendant un appel de la passerelle. La tonalité de déconnexion est spécifiée dans le paramètre Disconnect Tone, qui dépend de la région du service RTPC. La valeur par défaut est yes.

Disconnect Tone	Cette valeur correspond au script de tonalité qui permet au SPA de détecter la tonalité comme une tonalité de déconnexion. La syntaxe suit un script de tonalité standard avec quelques restrictions. La valeur par défaut est la tonalité de réorganisation (ligne occupée rapide) standard aux États-Unis, pendant 4 secondes. Restrictions : ▪ 2 composants de la fréquence doivent être indiqués. Si vous désirez une fréquence unique, la même fréquence est utilisée pour les deux composants. ▪ La valeur du niveau de la tonalité n'est pas utilisée. La valeur –30 dBm doit être utilisée pour le moment. ▪ Un seul ensemble de segments est autorisé. ▪ La durée totale de l'ensemble de segments est interprétée comme la durée minimale de la tonalité pour déclencher la détection. ▪ 6 segments de temps de fonctionnement et d'arrêt peuvent être spécifiés. Une marge de 10 % est utilisée pour valider les caractéristiques de la cadence de la tonalité. Les valeurs suivantes correspondent aux scripts de tonalité de déconnexion pour différents pays : **US** (par défaut) — 480@-30, 620@-30;4 (.25/.25/1+2) **UK** : 400@-30,400@-30; 2(3/0/1+2) **France** : 440@-30,440@-30; 2(0.5/0.5/1+2) **Germany—**425@-10; 10(0.48/0.48/1) **Netherlands** : 425@-30,425@-30; 2(0.5/0.5/1+2) **Sweden** : 425@-10; 10(0.25/0.25/1) **Norway** : 425@-10; 10(0.5/0.5/1) **Italy** : 425@-30,425@-30; 2(0.2/0.2/1+2) **Spain** : 425@-10; 10(0.2/0.2/1,0.2/0.2/1,0.2/0.6/1) **Portugal** : 425@-10; 10(0.5/0.5/1) **Poland** : 425@-10; 10(0.5/0.5/1) **Denmark** : 425@-10; 10(0.25/0.25/1) **New Zealand** : 400@-15; 10(0.25/0.25/1) **Australia** : 425@-13; 10(0.375/0.375/1)

Paramètres internationaux

Voice > PSTN > International Settings

FXO Country Setting	Sélectionnez le pays du déploiement dans la liste déroulante.5
FXO Port Impedance	Permet de configurer l'impédance souhaitée pour le port FXO. Options disponibles : {**600**, **900, 270+750||150nF, 220+820||120nF**, **370+620||310nF**, **320+1050|| 230nF**, **370+820||110nf**, **275+780||115nF**, **120+820||110nF**, **350+100 || 210nF**, **0 + 90 ||130nF**}, **600+2.16uF**, **900+1uF, 900+2.16uF, 6001uF,** ou **Global.** La valeur par défaut est 600. Les valeurs d'impédance suivantes correspondent à différents pays : **US** : 600 **EU (UK, France, Germany, Netherlands, Sweden, Norway, Italy, Spain, Portugal, Poland, and Denmark)** : 270+750||150nF Australia : 220+820||120nF New Zealand : 370+620||310nF
CO (Device) Termination	Spécifiez la valeur de terminaison de périphérique. Options disponibles : **Unknown**, **900+2.16uF**, **600,1200+376 ||112nf**, **150+510||150nF, 600||15uF**, **220+120||115nF**, **220+820||115nF**, **370 + 620||310nF**, **220+820||120nF**, **300+1000|| 270+750||150nF, 200+560||100nF**
Line Type	Spécifiez le type de ligne. Options disponibles : EIA (0-7), 2000 ft. et 22, 24 ou 26 awg.
Impedance Match	Détermine le meilleur paramètre de correspondance d'impédance pour le port FXO ou FXS. La valeur par défaut est no.
Ring Frequency Min	Permet de spécifier la plus basse limite de la fréquence de sonnerie utilisée pour détecter le signal de sonnerie. La valeur par défaut est 10.
SRP To PSTN Gain	dB de gain numérique (ou d'atténuation s'il est négatif) à appliquer au signal envoyé par la SRP au PSTN. Plage de valeurs comprises entre 15 et 12. La valeur par défaut est 0.

Ring Frequency Max	Permet de spécifier la limite la plus élevée de la fréquence de sonnerie utilisée pour détecter le signal de sonnerie. La valeur par défaut est 100.
PSTN To SRP Gain	dB de gain numérique (ou d'atténuation s'il est négatif) à appliquer au signal envoyé par le PSTN à la SRP. La plage est comprise entre - 15 et 12. La valeur par défaut est 0.
Ring Validation Time	Permet de spécifier la durée minimale du signal nécessaire à la SRP pour le reconnaître comme un signal de sonnerie. La valeur par défaut est 256 ms.
Tip/Ring Voltage Adjust	Les options disponibles sont {3.1V, 3.2V, 3.35V, 3.5V}. La valeur par défaut est 3.5V.
Ring Indication Delay	Choisissez entre {0, 256, 512, 768, 1024, 1280, 1536, 1792} (ms). La valeur par défaut est 512 ms.
Operational Loop Current Min	Les options possibles sont les suivantes (mA) : {10, 12, 14, 16). La valeur par défaut est 10.
Ring Timeout	Choisissez entre {0, 128, 256, 384, 512, 640, 768, 896, 1 024, 1 152, 1 280, 1 408, 1 536, 1 664, 1 792, 1 920} (ms). La valeur par défaut est 640 ms.
On-Hook Speed	Choisissez entre {Less than 0.5ms, 3ms (ETSI), 26ms (Australia)}. La valeur par défaut est Less than 0.5 ms.
Ring Threshold	Choisissez entre {13.5–16.5, 19.35–23.65, 40.5–49.5} (Vrms). La plage par défaut est 13.5-16.5 Vrms.
Current Limiting Enable	Permet d'activer ou de désactiver le limitateur électrique. La valeur par défaut est no.
Ring Frequency Min	Fréquence de sonnerie minimale à détecter. La plage est comprise entre 5 et 100. La valeur par défaut est 10.
Ring Frequency Max	Fréquence de sonnerie maximale à détecter. La plage est comprise entre 5 et 100. La valeur par défaut est 100.

Ring Validation Time	Choisissez entre {100, 150, 200, 256, 384, 512, 640, 1 024} (ms.) La valeur par défaut est 256ms.
Ringer Impedance	Choisissez entre {High, Synthesized (Poland, S.Africa, Slovenia)}. La valeur par défaut est high.
Line-In-Use Voltage	Permet de déterminer le seuil de tension, à partir duquel la SRP peut supposer que le PSTN est utilisé par un autre combiné partageant la même ligne (et déclarer le service de passerelle PSTNcomme indisponible pour les appels entrants VoIP). La valeur par défaut est 30v.

Pages User

Utilisez ces pages pour configurer les paramètres utilisateur de l'appelant.

REMARQUE Selon votre numéro de modèle, le nombre de pages utilisateur disponibles peut varier. Étant donné que les modèles de SRP520-U prennent uniquement en charge 2 lignes (Line 1 et Line 2), seules deux pages User s'afficheront (User 1 et User 2).

Ces pages incluent les sections suivantes :

- **Paramètres de transfert d'appel**
- **Paramètres de transfert d'appel sélectif**
- **Paramètres de numérotation abrégée**
- **Paramètres de service supplémentaire**
- **Paramètres de sonnerie distincts**
- **Paramètres de sonnerie**

Lorsqu'un appel est effectué à partir de l'une des lignes disponibles, la SRP utilise les paramètres d'utilisateur et de ligne pour cette ligne ; il n'y a pas de prise en charge de la connexion utilisateur. [1], [2], [3] ou [4] (correspondant à la ligne appropriée) doit être ajouté aux balises des paramètres utilisateur dans le profil de configuration. Ces caractères sont omis ci-dessous pour une meilleure lisibilité.

Paramètres de transfert d'appel

Voice > User 1–4 > Call Forward Settings

Cfwd All Dest	Numéro de renvoi du service de transfert de tous les appels. Par défaut, cette valeur n'est pas définie.
Cfwd Busy Dest	Numéro de renvoi du service de transfert d'appel si occupé. Par défaut, cette valeur n'est pas définie.
Cfwd No Ans Dest	Numéro de renvoi du service de transfert d'appel si pas de réponse. Par défaut, cette valeur n'est pas définie.
Cfwd No Ans Delay	Délai en seconde avant le déclenchement du transfert d'appel en l'absence de réponse La valeur par défaut est 20.

Paramètres de transfert d'appel sélectif

Voice > User 1-4 > Selective Call Forward Settings

Cfwd Sel1- 8 Caller	Modèle de numéro permettant de déclencher le transfert d'appels sélectif 1, 2, 3, 4, 5, 6, 7 ou 8. Par défaut, cette valeur n'est pas définie.
Cfwd Sel1 - 8 Dest	Numéro de renvoi pour le transfert d'appels sélectif 1, 2, 3, 4, 5, 6, 7 ou 8. Par défaut, cette valeur n'est pas définie.
Cfwd Last Caller	Numéro d'appelant transféré de manière active vers Cfwd Last Dest à l'aide du code d'activation Call Forward Last Par défaut, cette valeur n'est pas définie.
Cfwd Last Dest	Numéro de transfert du paramètre Cfwd Last Caller. Par défaut, cette valeur n'est pas définie.
Block Last Caller	IDde l'appelant bloqué via le service Block Last Caller. Par défaut, cette valeur n'est pas définie.
Accept Last Caller	ID de l'appelant accepté via le service Accept Last Caller. Par défaut, cette valeur n'est pas définie.

Paramètres de numérotation abrégée

Voice > User 1-4 > Speed Dial Settings

Speed Dial 2-9	Numéro de téléphone cible (ou URL) attribué à la numérotation rapide 2, 3, 4, 5, 6, 7, 8 ou 9. Par défaut, cette valeur n'est pas définie.

Paramètres de service supplémentaire

La SRP offre une prise en charge native de nombreux services avancés ou supplémentaires. Tous ces services sont facultatifs. Les paramètres figurant dans le tableau ci-dessous permettent d'activer ou de désactiver un service supplémentaire spécifique. Un service supplémentaire doit être désactivé si a) l'utilisateur n'y a pas souscrit ou b) le fournisseur d'accès prend en charge un service similaire en utilisant un autre équipement que la SRP.

Voice > User 1-4 > Supplementary Service Settings

CW Setting	Appel en attente (activé/désactivé) pour tous les appels. La valeur par défaut est yes.
Block CID Setting	Blocage de l'ID de l'appelant (activé/désactivé) pour tous les appels. La valeur par défaut est no.
Block ANC Setting	Blocage des appels anonymes (activé/désactivé). La valeur par défaut est no.
DND Setting	DND (activé/désactivé). La valeur par défaut est no.
CID Setting	Génération de l'ID de l'appelant (activé/désactivé). La valeur par défaut est yes.
CWCID Setting	Gérération de l'ID de l'appelant pour les appels en attente (activé/désactivé). La valeur par défaut est yes.
Dist Ring Setting	Sonnerie distincte (activé/désactivé). La valeur par défaut est yes.

Secure Call Setting	Si ce paramètre est réglé sur yes, tous les appels sortants sont sécurisés par défaut. La valeur par défaut est no.
Message Waiting	L'utilisateur peut également la modifier manuellement pour effacer ou régler l'indicateur. Le réglage de cette valeur sur yes permet d'activer une tonalité saccadée ou un signal VMWI. Ce paramètre est stocké dans la mémoire à long terme et il subsiste après le redémarrage ou la mise hors tension. La valeur par défaut est no.
Accept Media Loopback Request	Permet de contrôler la gestion des requêtes entrantes pour l'opération de rebouclage. Options disponibles : **Never**, **Automatic** et **Manual**, où : **never** : n'accepte jamais les appels en rebouclage ; envoi d'une réponse 486 à l'appelant **automatic** : accepte automatiquement l'appel sans émettre de sonnerie. **manual** : fait sonner le téléphone, l'appel doit être décroché manuellement avant le démarrage du bouclage. La valeur par défaut est Automatic.
Media Loopback Mode	Mode de rebouclage à appliquer localement lors de l'émission d'un appel pour demander un rebouclage multimédia. Options disponibles : **Source** et **Mirror.** La valeur par défaut est Source. Si la SRP répond à l'appel, le mode est déterminé par l'appelant.
Media Loopback Type	Type de rebouclage à utiliser lors de l'émission d'un appel pour demander un rebouclage multimédia. Les choix sont **Media** et **Packet**. La valeur par défaut est Media. **REMARQUE** Si la SRP répond à l'appel, le type de bouclage est alors choisi par l'appelant (la SRP choisit toujours le premier type de bouclage si l'offre en contient plusieurs).

Paramètres de sonnerie distincts

Les modèles de numéro de l'appelant sont mis en correspondance de la sonnerie 1 à la sonnerie 8. La première correspondance (pas la correspondance la plus proche) est utilisée pour avertir l'abonné.

Voice > User > Distinctive Ring Settings

Ring1 - 8 Caller	Modèle de numéro de l'appelant pour émettre une sonnerie distinctive/CWT 1, 2, 3, 4, 5, 6, 7 ou 8. Par défaut, cette valeur n'est pas définie.

Paramètres de sonnerie

Voice > User 1-4 > Ring Settings

Default Ring	Modèle de sonnerie par défaut (1 à 8) pour tous les appelants. La valeur par défaut est 1.
Default CWT	Modèle CWT par défaut (1 à 8) pour tous les appelants. La valeur par défaut est 1.
Hold Reminder Ring	Modèle de sonnerie pour le rappel d'un appel en attente lorsque le téléphone est raccroché. La valeur par défaut est 8.
Call Back Ring	Modèle de sonnerie pour une notification de rappel. 7 constitue la valeur définie par défaut.

7

Configuration VPN

Ce chapitre décrit la configuration des stratégies VPN et des paramètres de la gamme SRP. Il comprend les sections suivantes :

- **VPN IPSec de site à site**
- **Tunnel GRE**
- **Transfert VPN**
- **Serveur Cisco VPN**

Pour accéder à ces pages, cliquez sur **VPN** dans la barre de menu de l'utilitaire de configuration.

VPN IPSec de site à site

Cette section décrit comment configurer les paramètres VPN pour permettre à d'autres sites de se connecter au réseau. Elle comprend les rubriques suivantes :

- **Page NAT Traversal**
- **Page IKE Policy**
- **Page IPSec Policy**

Page NAT Traversal

Si le modèle SRP ou tout homologue IPSec se trouve derrière un périphérique de traduction d'adresses réseau, activez la méthode NAT Traversal IPSec pour détecter et localiser la traduction. Afin de maintenir le tunnel, le trafic actif est alors généré conformément à la disposition RFC3947.

ÉTAPE 1 Cliquez sur **VPN > Site-to-Site IPSec VPN > NAT Traversal**. La fenêtre NAT Traversal s'ouvre.

ÉTAPE 2 Pour activer la fonctionnalité NAT Traversal, sélectionnez **Enabled**. Cette option est désactivée par défaut.

ÉTAPE 3 Cliquez sur **Submit** pour enregistrer les modifications.

Page IKE Policy

Utilisez la page IKE Policy pour configurer une stratégie IKE VPN. Chaque stratégie IKE contient les paramètres permettant de définir des règles d'authentification IKE. Ces stratégies IKE peuvent être utilisées dans différentes stratégies VPN.

ÉTAPE 1 Cliquez sur **VPN > Site to Site IPSec VPN > IKE Policy**. La fenêtre IKE Policy s'ouvre. Cette fenêtre vous permet d'afficher les stratégies existantes, de modifier une stratégie ou d'ajouter une nouvelle stratégie IKE.

ÉTAPE 2 Pour ajouter une stratégie IKE, cliquez sur **Add Entry**. La fenêtre de configuration des stratégies IKE s'ouvre pour configurer la nouvelle stratégie.

ÉTAPE 3 Dans le champ **Policy Name**, entrez un nom unique pour la stratégie VPN.

ÉTAPE 4 Sélectionnez un mode d'échange dans la liste déroulante. Sélectionnez le mode **Main** pour une sécurité plus élevée au détriment de la vitesse de connexion. Sélectionnez le mode **Aggressive** pour bénéficier d'une connexion plus rapide au détriment de la sécurité.

ÉTAPE 5 Définissez les paramètres IKE SA appropriés qui figurent dans le tableau **Paramètres de la stratégie IKE** ci-dessous.

ÉTAPE 6 Si vous êtes connecté à un serveur XAUTH, entrez respectivement un nom d'utilisateur et un mot de passe dans les champs **Username** et **Password**. Lorsqu'il est activé, le modèle SRP peut authentifier les utilisateurs d'un serveur d'authentification externe, tel qu'un serveur RADIUS.

ÉTAPE 7 Cliquez sur **Submit** pour enregistrer les paramètres.

Paramètres de la stratégie IKE

Généralités	
Policy Name	Entrez un nom unique pour la stratégie VPN.
Exchange Mode	Définissez les paramètres de configuration de base pour la sécurité et la vitesse. **Main** : Fournit une sécurité plus élevée au détriment de la vitesse de connexion. Le mode principal dépend des échanges de clés bidirectionnels entre l'initiateur et le destinataire. Le processus d'échange de clés ralentit la connexion, mais augmente la sécurité. **Aggressive** : Fournit une connexion plus rapide au détriment de la sécurité. En mode agressif, les échanges de clés entre l'initiateur et le destinataire sont moins nombreux. Les deux parties échangent des informations ; cet échange est antérieur à l'existence d'un canal sécurisé.
Local ID and Remote ID	Saisissez les identifiants locaux et distants nécessaires à l'utilisation de la phase 1 de la négociation IKE ou laissez ces champs vides pour ignorer les paramètres d'identification. Options disponibles : ▪ IP address (par exemple : 1.1.1.1) ▪ User Specified Name: FQDN (précédé de l'**arobase** @) qui signifie qu'il ne doit pas être résolu. Par exemple : @www.cisco.com
Paramètres de la stratégie IKE SA	
Encryption Algorithm	Mode de cryptage. Sélectionnez entre **DES**, **3DES**, **AES128**, **AES192** et **AES256**.
Authentication Algorithm	Algorithme d'authentification pour les paramètres IKE SA. Sélectionnez **MD5** ou **SHA1**.
Diffie-Hellman (DH) Group	Groupe DH (Diffie-Hellman) permettant de définir la puissance de l'algorithme dans les bits. Sélectionnez **Group 1 (768 bit)** ou **Group 2 (1024 bit).**
Pre Shared Key	Entrez une clé alphanumérique à partager avec l'homologue IKE.

Paramètres de la stratégie IKE

Enable Dead Peer (DPD) Detection	Pour activer la détection DPD, sélectionnez **Enable**. La valeur par défaut est Disable. La détection DPD n'est pas requise pour une règle IKE, mais si cette fonction est activée, elle permet de conserver la connexion active lors des périodes sans trafic.
DPD Interval	Entrez un intervalle pour la détection DPD. En l'absence de trafic de données, ce paquet est régulièrement envoyé par intervalle de secondes.
DPD Timeout	Entrez un délai d'expiration (en secondes) pour la détection DPD.
Authentification étendue	
XAUTH Client Enable	Sélectionnez **Enable** si l'homologue VPN requiert des identifiants pour l'authentification étendue. La valeur par défaut est Disable.
Username/ Password	Entrez les identifiants que le modèle SRP utilise pour se connecter à l'homologue distant.

Page IPSec Policy

Utilisez la page IPSec Policy pour configurer une stratégie IPSec VPN. La stratégie VPN IPSec contient les paramètres d'association de sécurité IPSec qui définissent le type de connexion et de clé.

ÉTAPE 1 Cliquez sur **VPN > Site to Site IPSec VPN > IPSec Policy**. La fenêtre IPSec Policy s'ouvre. À partir de cette page, vous pouvez afficher les stratégies IPSec existantes, modifier une stratégie IPSec ou en ajouter une. Vous pouvez également afficher les informations détaillées de chaque stratégie dans le tableau des détails IPSec.

ÉTAPE 2 Pour ajouter une stratégie IPSec, cliquez sur **Add Entry**. Une nouvelle fenêtre IPSec Policy s'ouvre.

ÉTAPE 3 Pour activer la nouvelle stratégie, sélectionnez **Enable**.

ÉTAPE 4 Choisissez un numéro d'identification de stratégie dans la zone de liste déroulante **Policy Number**.

ÉTAPE 5 Dans le champ **Policy Name**, entrez un nom unique pour la stratégie IPSec.

ÉTAPE 6 Sélectionnez un type de stratégie dans la liste déroulante. Sélectionnez **Auto Policy** ou **Manual Policy**.

ÉTAPE 7 Entrez les paramètres de stratégie IPSec comme définis dans le tableau **Paramètres de la stratégie IPSec** ci-dessous.

ÉTAPE 8 Cliquez sur **Submit** pour enregistrer les paramètres.

La stratégie IKE apparaît dans le tableau List of IKE policies de la page IKE Policy Add Entry. Pour afficher les stratégies, cliquez sur le bouton **View IKE Table**.

Paramètres de la stratégie IPSec

Paramètres généraux	
Enable	Cochez la case pour activer la stratégie.
Policy Number	Saisissez un numéro d'identification pour la stratégie.
Policy Name	Entrez un nom unique pour la stratégie.
Policy Type	Sélectionnez le type de stratégie. Sélectionnez **Auto Policy** ou **Manual** Policy. La stratégie automatique utilise le protocole IKE pour négocier les clés aléatoires pour plus de sécurité. Si vous choisissez cette option, vous devez également définir une stratégie IKE sur la page **Site to Site IPSec VPN > IKE Policy**. La stratégie manuelle n'est pas de type IKE, ce qui en fait une stratégie plus simple, mais moins sécurisée.
Remote Endpoint	Choisissez le mode d'identification de la passerelle distante pour ce tunnel VPN de site à site. Sélectionnez **IP Address** pour saisir une adresse IP, sélectionnez **FQDN** pour saisir un nom de domaine complet ou sélectionnez **Any** (uniquement disponible dans le cadre d'une stratégie automatique). Notez bien qu'un nom de domaine complet implique la connexion du modèle SRP à un serveur DNS pour résoudre l'adresse avant d'établir le tunnel VPN.
Encryption Algorithm	Choisissez l'algorithme de cryptage. Sélectionnez **DES 3DES**, **AES128, AES192** ou **AES256**.
Integrity Algorithm	Choisissez un algorithme d'authentification. Sélectionnez **MD5** ou **SHA-1**.

Paramètres de la stratégie IPSec

WAN Interface Name	Choisissez l'interface WAN qui doit être utilisée pour la connexion à la passerelle distante pour ce tunnel VPN de site à site. La valeur par défaut est System Default.
Paramètres de la stratégie automatique (ces options s'affichent uniquement si la stratégie automatique est sélectionnée)	
PFS	Sélectionnez **Enable** pour activer le protocole PFS (Perfect Forward Secrecy). Cette option est désactivée par défaut. Cette fonctionnalité requiert un nouvel échange Diffie-Hellman pour chaque négociation de phase 2. Même si ce processus est plus lent, il garantit qu'aucune clé ne dépend d'aucune autre clé utilisée précédemment.
SA Lifetime	Entrez la durée de vie d'une stratégie IPSec SA en secondes. La valeur par défaut est 7 800 sec. (130 mn). La plage s'étend entre 60 et 28 800 secondes.
Paramètres de stratégie manuelle (ces options s'affichent uniquement si la stratégie manuelle est sélectionnée)	
SPI Incoming	Entrez une valeur hexadécimale dans la zone d'index des paramètres de sécurité entrants Security Parameters Index qui soit comprise entre 0x100 et 0xffffffff.
SPI Outgoing	Entrez une valeur hexadécimale dans la zone d'index des paramètres de sécurité sortants Security Parameters Index qui soit comprise entre 0x100 et 0xffffffff.
Encryption Algorithm Key	Entrez une valeur hexadécimale pour la clé d'algorithme de cryptage. La longueur dépend de l'algorithme de cryptage que vous avez sélectionné. Options disponibles : DES :16 caractères, 3DES : 48 caractères, AES-128 : 32 caractères, AES-192 : 48 caractères, AES-256 : 64 caractères.
Integrity Algorithm Key	Entrez une valeur hexadécimale pour la clé d'algorithme d'intégrité. La longueur de la clé dépend de l'algorithme d'intégrité sélectionné. Options disponibles : MD5: 32 caractères, SHA-1 : 40 caractères.

Paramètres de la stratégie IPSec

Sélection du trafic local	
Local IP	Détermine les hôtes locaux autorisés à utiliser la stratégie VPN. Sélectionnez **IP Address** ou un **sous-réseau** (adresse IP et masque de sous-réseau).
Sélection du trafic à distance	
Remote IP	Le trafic des hôtes locaux autorisés vers l'adresse IP ou le sous-réseau distant est routé via le tunnel VPN. Sélectionnez une adresse IP unique **IP Address** ou un masque de sous-réseau **Subnet**.
Select IKE Policy	Choisissez une stratégie IKE à associer à cette stratégie IPSec. Pour afficher toutes les stratégies IKE, cliquez sur le bouton **View IKE Table**.

Tunnel GRE

Utilisez la page Tunnel GRE pour configurer l'encapsulation GRE (Generic Routing Encapsulation). L'encapsulation GRE est un protocole de tunnellisation développé par Cisco qui peut encapsuler des types de paquets du protocole de couche réseau à l'intérieur des tunnels IP, créant ainsi une liaison point à point virtuelle au modèle SRP à des points distants sur un inter-réseau IP.

ÉTAPE 1 Cliquez sur **VPN > Site to Site IPSec VPN > GRE Tunnel**. La fenêtre GRE Tunnel s'ouvre. À partir de cette page, vous pouvez afficher les tunnels GRE existants, modifier un tunnel GRE ou en ajouter un nouveau. Vous pouvez également afficher les informations détaillées de chaque tunnel dans le tableau des détails GRE.

ÉTAPE 2 Pour ajouter un tunnel GRE, cliquez sur **Add Entry**. La fenêtre GRE IP Tunnel s'ouvre.

ÉTAPE 3 Choisissez un nombre de tunnels et entrez un nom de tunnel.

ÉTAPE 4 Pour activer le tunnel, cochez la case **Enable**.

ÉTAPE 5 Indiquez les paramètres pour la somme de contrôle, l'ordre et la clé comme défini dans le tableau **Paramètres de tunnel GRE ci-dessous.**

ÉTAPE 6 Choisissez l'interface WAN via laquelle le tunnel doit être connecté. Par exemple : WAN1 ou WAN2. System Default Route est le paramètre par défaut.

ÉTAPE 7 Entrez l'adresse IP de destination du périphérique distant qui terminera le nouveau tunnel.

ÉTAPE 8 Entrez l'adresse IP et le masque de sous-réseau de l'hôte distant. Cliquez sur le bouton **Add** pour ajouter d'autres adresses IP ou sur **Delete** pour en supprimer une.

ÉTAPE 9 Cliquez sur **Submit** pour enregistrer les paramètres.

Paramètres de tunnel GRE

Tunnel Number	Choisissez un numéro d'identification pour ce tunnel. Vous pouvez créer jusqu'à 10 tunnels.
Tunnel Name	Entrez un nom pour décrire ce tunnel.
Enable	Cochez cette case pour activer le tunnel ou décochez-la pour le désactiver.
Checksum	Sélectionnez **Input**, **Output**, **Both** ou **None**. La valeur par défaut est Aucun. L'entrée nécessite que tous les paquets entrants disposent de la somme de contrôle appropriée. La sortie requiert les sommes de contrôle pour les paquets sortants. Les deux requièrent la somme de contrôle pour tous les paquets entrants et sortants.
Sequence	Choisissez **None**, **Both**, **Input** ou **Output**. La valeur par défaut est Aucun. La sortie requiert le numéro de séquence pour les paquets sortants. L'entrée requiert le numéro de séquence pour les paquets entrants. Les deux requièrent un numéro de séquence pour les paquets entrants et sortants.
Key	Sélectionnez les valeurs **None**, **Both**, **Input** ou **Output**. La valeur par défaut est Aucun. Le paramètre d'entrée définit la clé pour l'entrée. Le paramètre de sortie définit la clé pour la sortie. Les deux définissent la clé à utiliser dans les deux sens.
Key value	Si vous avez choisi une clé, entrez sa valeur comprise entre 0 et 4 294 967 295.
WAN Interface Name	Choisissez l'interface WAN permettant de créer le tunnel GRE avec l'hôte distant.

Paramètres de tunnel GRE

Destination IP or HostName	Adresse IP ou nom de domaine complet du périphérique distant qui terminera le tunnel.
Remote IP Address/ Subnet Mask	Répertorie les hôtes et les réseaux distants disponibles via le tunnel.
Modify Remote IP Address/Subnet Mask	Pour définir un hôte ou un réseau accessible via le tunnel, entrez l'adresse et le masque de sous-réseau et cliquez sur **Add**. Pour supprimer une adresse, sélectionnez-la dans la liste des adresses IP à distance, puis cliquez sur **Delete**.

Transfert VPN

Utilisez la page VPN Passthrough pour configurer le transfert VPN pour les protocoles IPSec, PPTP et L2TP. Utilisez cette fonctionnalité s'il existe des périphériques derrière le modèle SRP qui ont besoin de tunnel IPSec pour être installés indépendamment, comme la connexion à un autre routeur sur le réseau WAN.

ÉTAPE 1 Cliquez sur **VPN > Site to Site IPSec VPN > VPN Passthrough**. La fenêtre VPN Passthrough s'ouvre.

ÉTAPE 2 Les transferts IPSec, PPTP et L2TP sont activés par défaut. Cliquez sur **Disabled** pour désactiver l'une de ces options de transfert.

ÉTAPE 3 Cliquez sur **Submit** pour enregistrer les paramètres.

Paramètres du transfert VPN

IPSec Passthrough (IPSec Pass-Thru)	Le protocole IPSec (Internet Protocol Security) désigne une série de protocoles utilisés pour sécuriser l'échange des paquets au niveau de la couche IP. L'option de transfert IPSec est activée par défaut. Pour la désactiver, sélectionnez **Disable**.
PPTP Passthrough (PPTP Pass-Thru)	Le protocole de tunnellisation point à point (PPTP) permet au protocole point à point d'être « tunnélisé » via un réseau IP. L'option PPTP PassThrough est activée par défaut. Pour la désactiver, sélectionnez **Disable**.

Paramètres du transfert VPN

Transfert L2TP	Le protocole L2TP (Layer 2 Tunneling Protocol) est la méthode utilisée pour activer des sessions point à point via Internet, au niveau de la couche 2. L'option L2TP PassThrough est activée par défaut. Pour la désactiver, sélectionnez **Disable**.

Serveur Cisco VPN

Cette section explique comment configurer les paramètres de stratégie du serveur Cisco VPN ainsi que ses utilisateurs. Le serveur Cisco VPN permet aux utilisateurs distants d'accéder aux ressources Intranet via un tunnel VPN IPSec en utilisant le Client VPN Cisco. Consultez le site www.cisco.com/go/vpnclient.

REMARQUE Seul le serveur VPN ou VPN de site à site peut être utilisé à la fois sur le modèle SRP. Si vous activez le serveur VPN, le serveur VPN de site à site est désactivé.

Configuration des groupes

Utilisez la page de groupe pour configurer les paramètres qui contrôlent le serveur Cisco VPN et les stratégies IPsec pour communiquer avec les utilisateurs distants.

ÉTAPE 1 Cliquez sur **VPN > Cisco VPN Server > Group**. La fenêtre Group s'ouvre.

ÉTAPE 2 Cliquez sur **Enable** pour activer le serveur VPN. La valeur par défaut est Disable.

ÉTAPE 3 Sous Identity, spécifiez respectivement le nom du groupe et le mot de passe dans les champs **Group Name** et **Password**.

ÉTAPE 4 Si nécessaire, modifiez les paramètres **IKE Phase 1** et **IKE Phase 2** pour respecter les stratégies IPSec souhaitées.

ÉTAPE 5 Indiquez les paramètres de configuration du mode.

REMARQUE : Les modèles SRP520 peuvent prendre en charge jusqu'à 5 connexions/affectations d'adresses IP simultanées. Quant aux modèles SRP54, ils peuvent en prendre jusqu'à 10.

a. Définissez le champ **DNS1** dans l'adresse du serveur DNS principal. Un serveur DNS de sauvegarde peut éventuellement être spécifié dans le champ **DNS2**.

b. Si nécessaire, indiquez les serveurs WINS à utiliser.

c. (Facultatif) Saisissez un message d'accueil dans le champ de la bannière. Ce message s'affiche à l'utilisateur final du client VPN une fois que la session VPN est établie.

ÉTAPE 6 Cliquez sur **Submit** pour enregistrer les paramètres.

Paramètres du serveur Cisco VPN

Groupe	
Enable	Cliquez sur **Enable** pour activer le serveur VPN. La valeur par défaut est Disable. **REMARQUE :** L'activation du serveur VPN désactive tous les tunnels VPN de site à site qui ont été définis.
identité	
Group Name	Entrez le nom du groupe Cisco VPN qui sera utilisé comme identifiant pour le serveur VPN. Ce nom doit correspondre au nom de groupe spécifié pour le profil de client VPN. Le nom peut contenir jusqu'à 32 caractères et respecter la casse.
Password	Saisissez le mot de passe du groupe Cisco VPN. Ce mot de passe doit correspondre au mot de passe du groupe spécifié pour le profil de client VPN. Le nom peut contenir jusqu'à 32 caractères et respecter la casse.
IKE Phase 1	
Aggressive Mode	Le mode agressif est appliqué par défaut et ne peut pas être modifié. Ce mode permet de négocier les associations de sécurité ISAKMP (SA) de la phase 1 à l'aide des clés pré-partagées pour l'authentification.

Paramètres du serveur Cisco VPN

ESP Algorithm	Saisissez un algorithme de cryptage pour ISAKMP SA. Options disponibles :AES. DES et 3DES. La valeur par défaut est AES.
AH Algorithm	Algorithme de hachage pour ISAKMP SA. Les options disponibles sont MD5 et SHA1. La valeur par défaut est MD5.
Auth Method	Méthode utilisée pour authentifier l'utilisateur distant. Les options disponibles sont **PSK** ou **PSK+XAUTH**. Si l'option PSK est sélectionnée, le client sera authentifié s'il indique le nom du groupe et le mot de passe appropriés. Si PSK+XAUTH est sélectionné, alors un nom d'utilisateur et un mot de passe supplémentaires sont requis.
DH Group	Le groupe Diffie-Hellman (DH) permet de définir la puissance de l'algorithme en bits. 2 modp [1024] est la seule option disponible.
IKE Phase 2P	
PFS Group	Options de groupe Diffie-Hellman pour PFS de la phase 2. Les choix possibles sont : 1 [modp 768], 2 [modp 1024], 5 [modp 1536], 14 [modp 2048] ou 15 [modp 3072].
SA Lifetime	Définit la durée d'utilisation d'une association de sécurité IPSec SA. La valeur par défaut est 30.
Mode de configuration	
IP Pool	**Starting IP Address** : Adresse IP de démarrage de la plage d'adresses qui sont attribuées au client distant. Cette plage ne doit pas être dans le même sous-réseau qu'un réseau VLAN. **Subnet Mask** : Sous-réseau pour la plage d'adresses attribuées aux clients distants. Le masque défini doit être suffisamment important pour s'adapter au nombre maximum de connexions prises en charge par votre modèle SRP.
DNS1	Serveur DNS principal utilisé par les clients distants.
DNS2	Serveur DNS secondaire utilisé par les clients distants.
WINS1	Serveur WINS principal utilisé par les clients distants.

Paramètres du serveur Cisco VPN

WINS2	Serveur WINS secondaire utilisé par les clients distants.
Banner	Message qui s'affiche à l'utilisateur distant après l'ouverture d'une session. La bannière peut contenir jusqu'à 500 caractères ASCII imprimables sur une ligne.

Page Users

La page Users contient une liste de noms d'utilisateur permettant de se connecter au serveur VPN SRP. Vous pouvez définir jusqu'à 15 utilisateurs uniques.

ÉTAPE 1 Cliquez sur **VPN > Cisco VPN Server > Users**. La fenêtre Users s'ouvre.

Cette page vous permet d'ajouter, de modifier ou de supprimer un compte d'utilisateur.

ÉTAPE 2 Pour ajouter un utilisateur, cliquez sur **Add Entry**. La page User Account s'ouvre.

ÉTAPE 3 Entrez un nom d'utilisateur pour le nouvel utilisateur dans le champ **Username**.

ÉTAPE 4 Spécifiez un mot de passe dans **Password** et réintroduisez-le dans le champ **Confirm Password** pour la confirmation.

ÉTAPE 5 Cliquez sur **Submit** pour enregistrer les paramètres.

L'utilisateur est ajouté au tableau List of VPN Server Users de la page Users.

ÉTAPE 6 Répétez les étapes 2 à 5 pour chaque utilisateur nécessitant un accès VPN.

User Account Settings

Username	Nom d'utilisateur que le client VPN doit fournir lors de l'utilisation de la méthode d'authentification PSK+XAUTH.
Password	Mot de passe que le client VPN doit fournir lors de l'utilisation de la méthode d'authentification PSK+XAUTH.
Confirm Password	Le contenu de ce champ doit correspondre au champ Password.

8

Paramètres d'administration

Ce chapitre décrit les paramètres d'administration des plates-formes prêtes à l'emploi. Il comprend les sections suivantes :

- Page Web Access Management
- Page Remote Support
- Gestion à distance
- Page Certificate Management
- Page Time Setup
- Gestion des utilisateurs
- Page User Privilege Control
- Consignation
- Page Factory Defaults
- Page Firmware Upgrade
- Sauvegarde et restauration des paramètres
- Page Reboot
- Paramètres de commutation
- Status

Pour accéder à ces pages, cliquez sur **Administration** dans la barre de menu de l'utilitaire de configuration.

Page Web Access Management

Utilisez la page Web Access Management pour configurer les paramètres d'accès web et les règles d'accès à distance pour le modèle SRP.

ÉTAPE 1 Cliquez sur **Administration > Web Access Management**. La fenêtre Web Access Management s'ouvre.

ÉTAPE 2 Si nécessaire, saisissez **Banner Text**. Il s'agit du texte que l'utilisateur verra lorsqu'il se connecte au modèle SRP. Vous pouvez saisir un maximum de 1 024 caractères.

ÉTAPE 3 Configurez les paramètres d'accès à distance définis dans le tableau **Paramètres de la gestion de l'accès au Web ci-dessous.**

ÉTAPE 4 Cliquez sur Submit pour enregistrer les paramètres.

Paramètres de la gestion de l'accès au Web	
Accès au Web	
Web Utility Access	Sélectionnez **HTTP** et/ou **HTTPS**. Pour un accès Internet sécurisé, sélectionnez **HTTPS**. Si vous sélectionnez HTTPS, vous devez inclure https à l'URL pour vous connecter à l'utilitaire. Par exemple : https://xxx.xxx.xxx.xxx, les x représentent l'adresse IP de la passerelle Internet.
Web Utility Access via Wireless	Permet aux périphériques associés au point d'accès sans fil SRP d'accéder à l'interface utilisateur Web. La valeur par défaut est Disabled.
Bannière d'ouverture de session	
Banner Text	Texte que l'utilisateur voit lorsqu'il accède à la page de connexion SRP. Vous pouvez saisir un maximum de 1 024 caractères.
Accès distant	
Remote Management	Permet de gérer votre modèle SRP à partir d'un site distant via Internet. La valeur par défaut est Disabled.

Paramètres de la gestion de l'accès au Web	
Web Utility Access	Sélectionnez **HTTP** ou **HTTPS**. Pour un accès Internet sécurisé, sélectionnez **HTTPS**. Pour HTTPS, entrez https://xxx.xxx.xxx.xxx (les x représentent l'adresse IP de la passerelle sur Internet) dans le champ de l'adresse de votre navigateur Web.
Remote Upgrade	Si cette fonction est activée, le microprogramme du modèle SRP peut être mis à niveau à partir d'Internet. **REMARQUE** Vous ne pouvez modifier ce paramètre qu'en vous connectant à l'interface Web du réseau LAN.
Allowed Remote IP Address	Pour accéder au modèle SRP à partir de n'importe quelle adresse IP externe, sélectionnez **Any IP Address**. Pour spécifier une adresse IP ou une gamme d'adresses IP externes, sélectionnez la deuxième case d'option et entrez la ou les adresses IP que vous souhaitez utiliser.
Remote Management Port	Entrez le numéro du port d'accès à distance. Le numéro de port par défaut est 8080.

Page Remote Support

Utilisez la page Remote Support pour aider les techniciens d'assistance Cisco à diagnostiquer les incidents techniques liés aux produits.

ÉTAPE 1 Cliquez sur **Administration > Remote Support**. La fenêtre Remote Support s'ouvre.

ÉTAPE 2 Cliquez sur le bouton **Collect Device Status Information** pour générer un aperçu de l'état opérationnel du modèle SRP dans un fichier nommé debug_info.tgz. Fournissez ce fichier directement à l'assistance technique de Cisco pour une analyse détaillée.

ÉTAPE 3 Si votre technicien d'assistance Cisco demande un accès à distance au modèle SRP pour diagnostiquer un incident technique, cochez la case **Enable Remote Support**.

ÉTAPE 4 Entrez un numéro de port d'accès dans le champ **Access Port** correspondant à l'interpréteur de commandes d'accès à distance.

ÉTAPE 5 Dans le champ **Remote Support Password**, saisissez un mot de passe défini en accord avec le technicien d'assistance. Vous devez également fournir au technicien l'adresse MAC du périphérique pour activer l'accès (voir Status > Router).

ÉTAPE 6 Cliquez sur **Submit** pour activer la session d'assistance à distance. Cette opération permet d'ouvrir un accès SSH sur le port spécifié pendant environ 30 minutes. Ensuite, l'accès distant est désactivé.

Paramètres d'assistance à distance	
Collect Device Status Information	Collecte les informations de configuration du système et de routage utiles pour le débogage de ce système.
Enable Remote assistance	Cochez cette case pour activer le shell de débogage à distance. Une fois activé, il est uniquement valable pendant 30 minutes.
Access Port	Numéro de port du shell de débogage.
Remote Support Password	Mot de passe d'assistance à distance.

Gestion à distance

Utilisez les pages Remote Management pour configurer les paramètres des éléments suivants :

- **Page TR-069**
- **Page SNMP**
- **Page Local TFTP**

Pour accéder à ces pages, cliquez sur **Administration > Remote Management** de l'utilitaire de configuration.

Page TR-069

Certains prestataires de services peuvent configurer automatiquement l'équipement des locaux du client à partir d'un serveur central. Utilisez la page TR-069 pour configurer la communication avec un serveur de configuration automatique (ACS).

ÉTAPE 1 Cliquez sur A**dministration > Remote Management > TR-069**. La fenêtre TR-069 s'ouvre.

ÉTAPE 2 Sélectionnez **Enabled** pour permettre la configuration automatique du modèle SRP à partir d'un serveur central. La valeur par défaut est Disabled.

ÉTAPE 3 Spécifiez les paramètres TR-069 tels qu'ils sont définis dans le tableau **Paramètres TR-069** ci-dessous.

ÉTAPE 4 Cliquez sur **Submit** pour enregistrer les paramètres.

Paramètres TR-069	
Status	Sélectionnez **Enabled** pour permettre la configuration automatique de votre routeur à partir d'un serveur central. La valeur par défaut est Disabled.
ACS URL	URL d'un serveur ACS fourni par votre prestataire de services. L'URL d'un serveur ACS est au format suivant : **Protocol://host:port/path** ▪ Le protocole peut être de type http ou https. ▪ L'hôte peut être un nom de domaine complet ou une adresse IP. ▪ Le port est facultatif. ▪ Le chemin dépend de la configuration du serveur ACS.
ACS Username	Saisissez un nom d'utilisateur dans le champ **Username** que le modèle SRP peut utiliser si le serveur ACS requiert une authentification. Le nom d'utilisateur par défaut est OUI-Numéro de série.

Paramètres TR-069	
ACS Password	Entrez un mot de passe dans le champ **Password** que le modèle SRP peut utiliser si le serveur ACS demande l'authentification.
Connection Request Port	Entrez le numéro du port de demande de connexion dans le champ **Connection Request Port** que le serveur ACS peut utiliser pour contacter le modèle SRP.
Connection Request Username	(Facultatif) Dans le champ **Username**, saisissez le nom d'utilisateur d'authentification que le serveur ACS doit utiliser lors d'une demande de connexion.
Connection Request Password	(Facultatif) Dans le champ **Password**, saisissez le mot de passe d'authentification que le serveur ACS doit utiliser lors d'une demande de connexion.
Periodic Inform Enable	Sélectionnez **Enabled** pour permettre au routeur d'envoyer régulièrement des messages au serveur ACS. Sinon, sélectionnez Disabled.
Periodic Inform Interval	Saisissez **Interval** (en secondes) lorsque le modèle SRP envoie un message d'information au serveur ACS. La valeur par défaut est de 86 400 secondes (24 heures).
Binding with Loopback Interface	Par défaut, tous les messages TR-069 sont associés à l'adresse IP WAN par défaut. Sinon, l'une des deux interfaces de bouclage SRP peut être utilisée pour les communications TR-069. En cas de sélection, le modèle SRP définit également son adresse URL de demande de connexion envoyée à l'aide de l'adresse de rebouclage.
Request Download	Cliquez sur le bouton **Apply** pour lancer immédiatement une connexion sur le serveur ACS. Le serveur ACS appelle le modèle RPC de téléchargement lorsqu'il reçoit la demande.
Provisioning Code	Entrez le code qui sera utilisé par un serveur ACS pour déterminer les paramètres personnalisés du fournisseur, ainsi que les paramètres de mise en service.

Page SNMP

SNMP est un protocole de surveillance et de gestion du réseau qui vous permet de surveiller et de gérer votre réseau à partir d'un gestionnaire SNMP. Le protocole SNMP permet de surveiller et de mettre des périphériques en réseau, de gérer les configurations, la collecte des statistiques, les performances et la sécurité. Le modèle SRP prend en charge les versions SNMP 1, 2 et 3.

ÉTAPE 1 Cliquez sur **Administration > Remote Management > SNMP**. La fenêtre SNMP s'ouvre.

ÉTAPE 2 Pour activer le SNMP, cliquez sur **Enabled**. La valeur par défaut est Disabled.

ÉTAPE 3 Saisissez les paramètres SNMP définis dans le tableau **Paramètres SNMP** ci-dessous.

ÉTAPE 4 Cliquez sur **Submit** pour enregistrer les paramètres.

Paramètres SNMP	
SNMP Enable/ Disable	Sélectionnez **Enabled** pour activer le protocole SNMP. La valeur par défaut est Disabled.
Trusted IP	Entrez l'adresse IP et le masque de sous-réseau d'un serveur de gestion ou d'un réseau pour accéder au modèle SRP via le protocole SNMP, ou choisissez **Any** pour autoriser l'accès à n'importe quelle adresse IP (non recommandé).
Get Community	Saisissez un mot de passe public qui permet l'accès en lecture seule aux informations SNMP du modèle SRP.
Set Community	Saisissez un mot de passe privé qui permet l'accès en lecture aux informations SNMP du modèle SRP.
SNMPv3	
SNMPv3 Enable/ Disable	Sélectionnez l'option **Enabled** pour activer SNMPv3. La valeur par défaut est Disabled, ce qui signifie que le protocole SNMPv2 est utilisé.
R/W User	Saisissez un nom d'utilisateur pour le protocole SNMPv3.
Auth-Protocol	Protocole d'authentification SNMPv3. Sélectionnez **HMAC-MD5** ou **HMAC-SHA** dans la liste déroulante.

Paramètres SNMP	
Auth-Password	Mot de passe d'authentification.
PrivProtocol	Protocole d'authentification pour la confidentialité. Choisissez **None** ou **CBC-DES** dans la liste déroulante. Si vous sélectionnez CBC-DES, le mot de passe de confidentialité permet de crypter la partie relative aux données du message qui est en cours d'envoi.
Privacy Password	Clé de cryptage utilisée par le protocole PrivProtocol.

Description des ports SNMP

Les tableaux suivants répertorient les étiquettes internes d'interface Linux utilisées par le protocole SNMP en répertoriant les interfaces.

Interfaces IP SRP500	
br0	Réseau WAN Ethernet 1
brn	Réseau LAN VLAN n, où n = 1-4079
br4080 through br4083	ADSL PVC1-4
br4088	Réseau WAN Ethernet 2
lo	Interface de bouclage. Adresses de gestion des hôtes configurés dans l'utilitaire de configuration et le bouclage interne (127.0.0.1).
ppp10	Interface PP de modem 3G
gre0 through gre9	Interface de tunnel GRE 1-10
ipsec0 through ipsec4	Interface de tunnel IPSec 1-5
ath0 through ath3	SSID1-4 sans fil

Interfaces internes SRP500	
eth0	Interface Ethernet WAN
eth1	Connexion interne au commutateur LAN
eth1.n	Connexion de sous-interface interne aux réseaux VLAN LAN. (" n " correspondant au numéro VLAN 1 - 4079)

Interfaces internes SRP500	
eth0.4080 through eth0.4083	Connexions en pont internes à la connexion ADSL PVC1-4
eth0.4093	Connexion interne au modem ADSL
wifi0	Connexion interne au point d'accès sans fil
ifb0	Non utilisé actuellement
ifb1	Non utilisé actuellement
mast0	Non utilisé actuellement

Page Local TFTP

Utilisez la page Local TFTP pour activer le modèle SRP en tant que serveur TFTP. Lorsque vous activez le serveur TFTP, vous pouvez charger des fichiers sur le modèle SRP distant, puis l'utiliser en tant que serveur local pour distribuer de petits fichiers vers des hôtes sur le réseau LAN, tels que des fichiers de configuration d'amorce pour les téléphones IP, notamment. L'espace de stockage local SRP pour le serveur TFTP est de 1 Mo.

ÉTAPE 1 Cliquez sur **Administration > Remote Management > Local TFTP**. La fenêtre Local TFTP Control s'ouvre.

ÉTAPE 2 TFTP est activée par défaut. Pour la désactiver, sélectionnez **Enabled**, puis cliquez sur **Submit**.

ÉTAPE 3 Indiquez les paramètres d'obtention des fichiers à distance dans le champ Get Remote File Settings comme indiqué dans le tableau **Paramètres TFTP locaux** ci-dessous pour charger vos fichiers.

Paramètres TFTP locaux	
TFTP	TFTP est activée par défaut. Pour la désactiver, sélectionnez **Disable**.
Paramètres d'obtention des fichiers à distance	
URL	Entrez l'URL de l'emplacement du fichier distant. Par exemple : http://www.votresite.com:port/chemin/nomdufichier ou ftp://nomutilisateur:motdepasse@votresite:port/chemin/nomdufichier.
Save As	Entrez le nom du fichier que vous enregistrez.
Session Timeout	Durée maximale fournie pour une session de connexion. Saisissez une valeur dans le champ **Session Timeout** (en secondes). La valeur par défaut est 10 secondes. ▪ La temporisation pour les sessions HTTP et FTP est égale à 3 secondes environ. ▪ La temporisation pour les sessions TFTP est égale à 1 seconde. **REMARQUE** Pour les sessions HTTP et FTP, un message de réponse de réinitialisation TCP doit mettre fin à la session.
Retry Sessions	Nombre de tentatives d'ouverture de sessions en cas de problème temporaire.
Get File	Cliquez sur ce bouton pour charger le fichier souhaité dans la liste de fichiers.
Status	État de traitement du fichier distant.
File List table	Affiche le nom et la taille du fichier distant.

Page Certificate Management

Si la mise en service TR-069 et XML est sécurisée par le protocole HTTPS, utilisez la page Certificate Management pour installer les certificats publics requis pour authentifier les serveurs de mise en service.

Les certificats numériques (également connus sous le nom de certificats PKI X.509 I) permettent d'authentifier l'identité des utilisateurs et des systèmes et sont émis par des autorités de certification comme Verisign ou Thawte. Chaque fichier de certificat peut inclure plusieurs certificats tant que la taille du fichier reste inférieure à 8 Ko.

ÉTAPE 1 Cliquez sur **Administration > Certificate Management.** La fenêtre Certificate Management s'ouvre.

Cette page répertorie les fichiers de certificat actuellement installés pour une utilisation avec les serveurs de mise en service TR-069 et XML. Cette page vous permet d'ajouter, de supprimer ou d'activer un fichier de certificat.

- Pour ajouter un fichier de certificat, entrez un nom descriptif dans la zone CA Name, puis cliquez sur **Choose File** ou **Browse** pour sélectionner le fichier de certificat (.pem). Cliquez sur le bouton **Upload** pour installer le fichier de certificat. Vous pouvez charger jusqu'à 3 fichiers de certificat pour une utilisation avec un serveur ACS TR-069, néanmoins, un seul fichier peut être activé à la fois.
- Pour supprimer un fichier de certificat actuellement installé, cliquez sur l'icône **Delete** (x) en regard du certificat à supprimer.
- Pour activer un fichier de certificat existant, cochez la case **Enable** en regard du certificat applicable.

ÉTAPE 2 Cliquez sur **Submit** pour enregistrer les paramètres.

Paramètres de gestion de certificat	
TR-069 Root CA File List	Répertorie le fichier de certificat disponible pour authentifier un serveur ACS TR-069.
Provision File List	Affiche le certificat disponible pour authentifier un serveur de mise en service XML.
Enabled	Cochez la case **Enable** pour activer un certificat. Décochez la case pour désactiver l'option.
CA Name	Saisissez un nom décrivant le certificat.
Select Certificate	Charge un certificat issu du PC client. Pour le charger, cliquez sur **Choose File** ou **Browse**, recherchez et sélectionnez le fichier de certificat (.pem), puis cliquez sur le bouton **Upload.** Pour supprimer un fichier de certificat actuellement installé, cliquez sur l'icône **Delete** (x) en regard du certificat à supprimer.

Page Time Setup

Utilisez la page Time Setup pour définir les paramètres du fuseau horaire de votre réseau. Vous pouvez configurer l'heure du système automatiquement ou à l'aide du serveur de protocole NTP (Network Time Protocol).

ÉTAPE 1 Cliquez sur **Administration > Time Setup**. La fenêtre Time Setup s'ouvre.

ÉTAPE 2 Choisissez le fuseau horaire de votre région dans la liste déroulante Time Zone. Le fuseau horaire fait souvent référence à l'heure locale.

ÉTAPE 3 Pour installer l'horloge du système manuellement, sous Manual Setting choisissez les paramètres **Date** et **Time**.

ÉTAPE 4 Pour définir l'heure à l'aide du serveur de protocole NTP, sélectionnez **NTP**. Spécifiez les paramètres NTP, tels qu'ils sont définis dans le tableau **Paramètres de configuration de l'heure** ci-dessous.

ÉTAPE 5 Pour récupérer l'heure système après un redémarrage du système, cochez la case **Auto Recovery After Reboot.** Par défaut, cette case est décochée.

ÉTAPE 6 Cliquez sur **Submit** pour enregistrer les paramètres.

Paramètres de configuration de l'heure
Fuseau horaire
Sélectionnez le fuseau horaire de votre région dans la liste déroulante. Par exemple : (GMT-8:00) Heure du Pacifique (États-Unis & Canada).
Manual Setting
Permet de régler l'horloge système manuellement. Saisissez la date sous "Jour/Mois/Année" et l'heure au format suivant : "Heure:Min.:Sec."

Paramètres de configuration de l'heure	
NTP	
Time Server Address	Définit l'heure à l'aide d'un serveur de protocole NTP. ▪ Pour régler automatiquement l'heure à l'aide des serveurs NTP par défaut du modèle SRP, choisissez **Auto.** Il s'agit du paramètre par défaut. ▪ Pour spécifier un serveur NTP particulier, sélectionnez **Manual** et saisissez le nom d'hôte ou l'adresse IP du serveur NTP.
Resync Timer	Saisissez le nombre de resynchronisations du modèle SRP avec le serveur NTP. La valeur par défaut est 3 600 secondes.
Enable Daylight Saving	Par défaut, l'heure d'été est activée. Pour la désactiver, décochez la case.
Auto Recovery After Reboot	
Cochez cette case pour récupérer l'heure système après un redémarrage du système. Par défaut, cette case est décochée. Après redémarrage, cette fonctionnalité tente de démarrer l'horloge du système pour qu'elle soit en conformité avec l'heure actuelle.	

Gestion des utilisateurs

La section décrit comment configurer les paramètres de gestion des utilisateurs pour authentifier et contrôler tous les utilisateurs qui se connectent au modèle SRP. Il comprend les sections suivantes :

- **Page Password Complexity Settings**
- **Page User List**

Page Password Complexity Settings

Utilisez la page Password Complexity Settings pour appliquer les exigences de complexité du mot de passe lors de sa création ou de sa modification. L'utilisation d'un mot de passe fort est la première ligne de défense contre les accès non-autorisés à votre réseau.

ÉTAPE 1 Cliquez sur **Administration > User Management > Password Complexity Settings**. La fenêtre Password Complexity Settings s'ouvre.

ÉTAPE 2 Par défaut, cette fonction est désactivée. Pour l'activer, cliquez sur **Enabled**.

ÉTAPE 3 Saisissez un mot de passe fort.

Le mot de passe doit comporter au minimum huit caractères et au moins trois des classes de caractères suivantes :

- A à Z (majuscules)
- a à z (minuscules)
- 0 à 9 (alphanumérique)
- caractères spéciaux (par exemple ! $ # %)

ÉTAPE 4 Cliquez sur **Submit** pour enregistrer les paramètres.

Page User List

Utilisez la page User List pour gérer les utilisateurs qui ont accès à l'utilitaire de configuration.

REMARQUE Le modèle SRP prend en charge deux comptes utilisateur, l'un pour l'administrateur et l'autre pour l'utilisateur restreint. Par défaut, ces comptes sont respectivement appelés "administrateur" et "Cisco ".

ÉTAPE 1 Cliquez sur **Administration > User Management > User List**. La fenêtre User List s'ouvre.

ÉTAPE 2 Cliquez sur l'icône **Edit** (stylo) pour le compte à modifier. La fenêtre User Account s'ouvre.

ÉTAPE 3 Spécifiez les paramètres utilisateur tels qu'ils sont définis dans le tableau **Paramètres de la liste d'utilisateurs** ci-dessous.

ÉTAPE 4 Cliquez sur **Submit** pour enregistrer les paramètres.

Paramètres de la liste d'utilisateurs	
Username	Entrez un nouveau nom d'utilisateur.
Old Password (Admin account only)	Saisissez votre ancien mot de passe. Il vous est demandé lorsque vous modifiez votre mot de passe.

Paramètres de la liste d'utilisateurs	
New Password/Confirm New Password	Entrez et confirmez un nouveau mot de passe. Le nombre maximal de caractères est fixé à 32. Le mot de passe par défaut du compte administrateur est **admin**. Le mot de passe invité par défaut est **cisco**. Il vous est demandé lorsque vous vous connectez à l'utilitaire de configuration. Pour des raisons de sécurité, nous vous recommandons vivement de le modifier. **REMARQUE** Si la fonctionnalité de complexité du mot de passe est activée, vous devez saisir un mot de passe fort composé de huit caractères minimum et d'au moins trois des classes de caractères suivantes : ▪ A à Z (majuscules) ▪ a à z (minuscules) ▪ 0 à 9 (alphanumérique) ▪ Caractères spéciaux : - _.
Level	Affiche le niveau des autorisations de cet utilisateur. Le compte d'administrateur a accès à tous les paramètres, tandis que le compte d'utilisateur a uniquement accès aux fonctionnalités définies dans la page User Privilege.

Page User Privilege Control

Utilisez la page Privilege Control pour spécifier les privilèges pour le compte d'utilisateur.

ÉTAPE 1 Cliquez sur **Administration > User Privilege Control**. La fenêtre User Privilege Control s'ouvre.

ÉTAPE 2 Choisissez l'un de ces types d'accès pour chaque fonctionnalité.

- **Read/Write** : permet au compte d'utilisateur d'afficher et de configurer la page Web.
- **Read Only** : permet au compte d'utilisateur d'afficher uniquement la page Web.
- **Hidden**: masque la page du compte d'utilisateur.

ÉTAPE 3 Cliquez sur **Apply** pour enregistrer les paramètres.

Consignation

Cette section décrit les options de consignation du modèle SRP. Il comprend les sections suivantes :

- **Page Log Setting**
- **Page Log module**
- **Page Log Viewer**
- **Page Firewall Log**

Pour accéder à ces pages, cliquez sur **Administration > Log** dans la barre de menu de l'utilitaire de configuration.

Page Log Setting

ÉTAPE 1 Cliquez sur **Administration > Log > Log Setting**. La fenêtre Log s'ouvre.

ÉTAPE 2 Entrez la taille de journal qui sera enregistrée dans la mémoire du modèle SRP. La plage autorisée s'étend de 128 à 1 024 Ko.

REMARQUE Si vous redémarrez le modèle SRP, ces messages de consignation ne sont pas enregistrés.

ÉTAPE 3 Pour enregistrer des messages système sur une carte mémoire USB connectée au modèle SRP, saisissez le nom du fichier à enregistrer au périphérique USB. La plage autorisée s'étend de 1 à 512 Mo. Si aucune carte mémoire USB n'est connectée, le message « USB disconnect » s'affiche.

ÉTAPE 4 Entrez respectivement les numéros d'adresse IP et de port pour le serveur syslog distant dans les champs **IP Address** et **Port**. Le port 514 désigne le port par défaut. La plage est comprise entre 1 et 65535.

ÉTAPE 5 Indiquez les paramètres de journal e-mail pour que les journaux soient envoyés à une adresse e-mail spécifique comme défini dans le tableau **Paramètres de consignation** ci-dessous.

ÉTAPE 6 Cliquez sur **Submit** pour enregistrer les paramètres.

Paramètres de consignation	
Local	Taille de journal enregistrée dans la mémoire du modèle SRP. La plage autorisée s'étend de 128 à 1 024 Ko.
USB	Pour enregistrer une liste de messages sur une carte mémoire USB qui est connectée au modèle SRP, saisissez le nom du fichier. La plage de taille de journal autorisée s'étend de 1 à 512 Mo. Si aucune carte mémoire USB n'est connectée, le message « USB disconnect » s'affiche.
Syslog Server	Adresse IP et numéro de port du serveur syslog distant. Le port 514 désigne le port par défaut. La plage est comprise entre 1–65535.
E-mail	
Sender and Receiver	Entrez l'adresse e-mail de l'expéditeur dans le champ **Sender** et du destinataire dans le champ **Receiver**.
SMTP Server	Saisissez l'adresse du serveur de messagerie SMTP dans le champ **SMTP Mail Server**.
SMTP Port	Dans le champ **SMTP Port**, entrez l'adresse du port SMTP correspondant au serveur d'écoute de messagerie. La valeur par défaut est le port 25.
Objet	Spécifiez un e-mail **Subject** pour les journaux.
Number of Logs	Entrez le nombre de journaux à collecter par e-mail dans le champ **Number of Logs**. La plage est comprise entre 10 et 200 journaux.
Interval	Saisissez la durée d'envoi d'email si la quantité de journaux n'atteint pas le nombre de journaux spécifiés. La plage valide est comprise entre 1 et 1 440 minutes.
User Name and Password	Remplissez les champs **User Name** et **Password** pour l'authentification du serveur de messagerie.

Page Log module

Utilisez les paramètres du module de consignation Log Module pour sélectionner le niveau de consignation des détails à collecter et leur lieu de destination.

ÉTAPE 1 Cliquez sur **Administration > Log > Log Module**. La fenêtre Log Module s'ouvre.

ÉTAPE 2 Pour collecter les journaux d'activité, sélectionnez **Enabled**. La valeur par défaut est Disabled. Lorsque la fonction de consignation est activée, vous pouvez choisir de collecter des messages relatifs au système et/ou au noyau.

ÉTAPE 3 Pour activer la consignation pour un service spécifique, cochez la case **Enable**.

ÉTAPE 4 Choisissez un niveau de priorité dans la liste déroulante **Priority level**. Ceux-ci sont décrits dans le tableau Logging Severity Settings à la **page 107**. Initialement, aucun journal n'est affiché tant que l'une de ces options n'est pas sélectionnée.

ÉTAPE 5 Cliquez sur **Submit** pour enregistrer les modifications.

Paramètres de module de consignation

Log Level	
Status	Pour collecter les journaux d'activité, sélectionnez **Enabled**. La valeur par défaut est Disabled.
Log	▪ Local : Enregistre le journal dans la mémoire système. ▪ USB : Enregistre le journal sur un périphérique USB. ▪ E-mail : Envoie le journal par e-mail. ▪ Syslog Server : Envoie le journal à un serveur de journaux spécifique. Pour configurer l'adresse du serveur, reportez-vous à la section **Page Log Setting, page 258**.

Page Log Viewer

ÉTAPE 1 Cliquez sur **Administration > Log > Log Viewer**. La fenêtre Log Viewer s'ouvre.

ÉTAPE 2 Cliquez sur le bouton **Download All Log** pour télécharger les messages de consignation dans un fichier de l'ordinateur local.

ÉTAPE 3 Cliquez sur le bouton **Clear Log** pour effacer tous les messages de consignation enregistrés dans la mémoire.

ÉTAPE 4 Sélectionnez le type de journaux à afficher sur la page Web de la liste déroulante Display. Vous pouvez sélectionner tous les journaux, **All**, les journaux du noyau, **kernel** ou les journaux du système, **system**. Initialement, aucun journal n'est affiché tant que l'une de ces options n'est pas sélectionnée.

ÉTAPE 5 Pour filtrer les messages de consignation à l'aide d'un modèle spécifique, entrez une chaîne appropriée dans le champ de filtre, puis cliquez sur le bouton **Filter** pour afficher tous les messages contenant ce modèle.

Par exemple, saisissez « [TR-069] » pour afficher tous les messages TR-069 dans la liste des journaux. Dans ce cas, vous devez configurer le journal pour capturer ces messages dans la fenêtre Log Module et configurer également le paramètre **All** dans la fenêtre Log Viewer pour afficher tous les messages. Voir aussi **Page Log module, page 260.**

Page Firewall Log

Utilisez la page Firewall Log pour sélectionner les préférences de consignation des événements de pare-feu.

ÉTAPE 1 Cliquez sur **Administration > Log > Firewall Log**. La fenêtre Firewall Log s'ouvre.

ÉTAPE 2 Cliquez sur **Enabled** pour activer la consignation de pare-feu. La valeur par défaut est Disabled.

ÉTAPE 3 Choisissez un niveau de gravité dans la liste déroulante Log Level comme défini dans le tableau **Paramètres de gravité de consignation ci-dessous. Tous les événements de ce niveau et des niveaux supérieurs sont consignés.**

ÉTAPE 4 Sélectionnez le module de pare-feu à consigner (attaque **SPI** ou **DoS**), puis saisissez le nombre d'événements à générer par journal.

ÉTAPE 5 Cliquez sur **Submit** pour enregistrer les modifications.

Paramètres de gravité de consignation

Log Level	
Emergency (level 0)	Système inutilisable. La définition syslog est LOG_EMERG.
Alert (level 1)	Intervention immédiate requise. La définition syslog est LOG_ALERT.
Critical (level 2)	La définition syslog est LOG_CRIT.

Paramètres de gravité de consignation

Error (level 3)	Erreurs. La définition syslog est LOG_ERR.
Warning (level 4)	Avertissements. La définition syslog est LOG_WARNING.
Notification (level 5)	Événement normal mais important. La définition syslog est LOG_NOTICE.
Information (level 6)	Message d'information uniquement. La définition syslog est LOG_INFO.
Debugging (level 7	Messages de débogage. La définition syslog est LOG_DEBUG.
Log Category	
SPI and DoS Attack	Sélectionnez le module de pare-feu à inspecter (pare-feu d'inspection des paquets (SPI, Stateful Packet Inspection), attaque DoS ou les deux) et saisissez le nombre d'événements à générer par journal.

Page Factory Defaults

Utilisez la page Factory Default pour rétablir les paramètres d'usine du modèle SRP.

REMARQUE Si le prestataire de services utilisait la fonctionnalité SP Defaults, alors ces paramètres de configuration sont rétablis à la place des paramètres d'usine par défaut Cisco.

ÉTAPE 1 Cliquez sur **Administration > Factory Defaults**. La fenêtre Factory Defaults s'ouvre.

ÉTAPE 2 Pour restaurer les paramètres d'usine du modèle SRP ou de la voix, sélectionnez **Yes**.

ATTENTION Sauvegardez tous les paramètres personnalisés des données (modèles SRP) ou de la voix que vous avez enregistrés. Ces paramètres personnalisés sont perdus lorsque les paramètres par défaut sont restaurés.

ÉTAPE 3 Cliquez sur **Submit** pour appliquer la réinitialisation.

Page Firmware Upgrade

Utilisez la page Firmware Upgrade pour mettre à niveau le microprogramme sur le modèle SRP.

REMARQUE Il n'est pas nécessaire de le mettre à niveau, sauf si vous rencontrez des difficultés avec le périphérique ou si le nouveau microprogramme dispose d'une fonctionnalité que vous souhaitez utiliser. Avant de procéder à la mise à niveau, nous vous recommandons de sauvegarder au préalable vos données. Pour obtenir plus d'informations, reportez-vous à la section **Page Backup Configuration, page 264.**

Pour télécharger le fichier de mise à niveau du microprogramme, accédez à : www.cisco.com/go/srp500. Cliquez sur le lien intitulé Download Software pour télécharger la dernière version du logiciel.

ÉTAPE 1 Cliquez sur **Administration > Firmware Upgrade**. La fenêtre Firmware Upgrade s'ouvre.

ÉTAPE 2 Cliquez sur Choose File ou Browse, puis sélectionnez l'emplacement du fichier de mise à niveau du microprogramme que vous avez téléchargé.

ÉTAPE 3 Cliquez sur le bouton **Upgrade**.

ATTENTION La mise à jour du microprogramme peut prendre quelques minutes. Tant que le processus n'est pas terminé, NE mettez PAS l'alimentation hors tension. N'appuyez PAS sur le bouton de réinitialisation du matériel et NE cliquez PAS sur le bouton Précédent de votre navigateur actuel.

Sauvegarde et restauration des paramètres

Cette section décrit comment sauvegarder et restaurer les paramètres de configuration du modèle SRP. Il comprend les sections suivantes :

- **Page Default Configuration**
- **Page Backup Configuration**
- **Page Restore Configuration**
- **Page Configuration XML**

Pour accéder à ces pages, cliquez sur **Administration > Backup & Restore** dans l'utilitaire de configuration.

Page Default Configuration

Utilisez la page Default Configuration pour spécifier les paramètres de configuration par défaut du modèle SRP.

REMARQUE Les valeurs par défaut du prestataire de services sont un ensemble spécifique de paramètres de configuration appliqués au modèle SRP lors du déploiement initial pour définir le comportement du périphérique après réinitialisation par le compte d'utilisateur. Ce paramètre définit l'utilisation ou non des valeurs par défaut du prestataire de services (ce qui permet à l'administrateur de restaurer les paramètres d'usine Cisco).

ÉTAPE 1 Cliquez sur **Administration > Backup & Restore > Default Configuration**. La fenêtre Default Configuration s'ouvre.

ÉTAPE 2 Sélectionnez **Yes** pour charger la configuration par défaut du prestataire de services. Sélectionnez **No** pour restaurer les paramètres d'usine par défaut Cisco sur le modèle SRP.

ÉTAPE 3 Cliquez sur **Submit** pour enregistrer les modifications.

Page Backup Configuration

Utilisez la page Backup Configuration pour sauvegarder les paramètres de configuration du modèle SRP dans un fichier. Vous pouvez restaurer ultérieurement ces mêmes paramètres sur le modèle SRP.

ÉTAPE 1 Cliquez sur **Administration > Backup & Restore > Backup Configuration**. La fenêtre Backup Configuration s'ouvre.

ÉTAPE 2 Cliquez sur le bouton **Backup** pour enregistrer les informations de configuration du modèle SRP.

Page Restore Configuration

Utilisez la page Restore Configuration pour restaurer les paramètres de configuration du modèle SRP à partir d'une sauvegarde précédente.

ÉTAPE 1 Cliquez sur **Administration > Backup & Restore > Restore Configuration**. La fenêtre Restore Configuration s'ouvre.

ÉTAPE 2 Cliquez sur **Choose File** ou **Browse** pour rechercher le fichier de sauvegarde, puis cliquez sur **Restore**.

Page Configuration XML

Pour des raisons de sécurité, lors de la sauvegarde et de la restauration de la configuration système via XML, il est important que tous les mots de passe soient protégés. Utilisez la page XML Configuration pour activer le cryptage et protéger le mot de passe dans le profil XML.

ÉTAPE 1 Cliquez sur **Administration > Backup & Restore > XML Configuration**. La fenêtre XML Configuration s'ouvre.

ÉTAPE 2 Le cryptage de mots de passe est activé par défaut. Pour le désactiver, décochez la case **Encrypt Password Text**.

ÉTAPE 3 Entrez la clé de cryptage dans la zone **Encryption Key**. Cette clé permet de crypter l'intégralité du mot de passe dans le fichier XML. Elle peut contenir jusqu'à 32 caractères et au moins trois des classes de caractères suivantes :

- A à Z (majuscules)
- a à z (minuscules)
- 0 à 9 (alphanumérique)
- Caractères spéciaux : - _.

REMARQUE Si ce champ est laissé vide, le mot de passe de la console de périphérique est utilisé. Pour obtenir le mot de passe de la console, contactez votre prestataire de services.

ÉTAPE 4 Cliquez sur **Submit** pour enregistrer les modifications.

Page Reboot

Utilisez la page Reboot pour redémarrer le modèle SRP (si nécessaire) à partir de l'utilitaire de configuration.

ÉTAPE 1 Cliquez sur **Administration > Reboot**. La fenêtre Reboot s'ouvre.

ÉTAPE 2 Cliquez sur le bouton **Reboot** pour réinitialiser le cycle du modèle SRP.

Paramètres de commutation

Cette section décrit comment configurer les paramètres de commutation pour le modèle SRP. Il comprend les sections suivantes :

- **Page Jumbo Setting**
- **Page Port Status**
- **Page DSL Switch Setting**
- **Page MAC Filtering (modèles SRP540 uniquement)**

Pour accéder à ces pages, cliquez sur **Administration > Switch Setting** dans l'utilitaire de configuration.

Page Jumbo Setting

Utilisez la page jumbo Setting pour définir une interface en mode Jumbo. Les trames Jumbo sont des trames Ethernet avec plus de 1 500 octets de la charge utile.

ÉTAPE 1 Cliquez sur **Administration > Switch Setting > Jumbo Setting**. La fenêtre Jumbo Setting s'ouvre. Cette page répertorie les interfaces (ports Ethernet physiques câblés) qui prennent en charge le mode Jumbo.

ÉTAPE 2 Pour modifier la taille de paquet, choisissez un mode dans la liste déroulante Jumbo Mode. La taille de paquet par défaut est de 2 048 octets. Vous pouvez également choisir entre 1 552, 2 048 ou 10 240 octets.

REMARQUE Les modèles SRP520-U prennent uniquement en charge 1 552 et 2 048 octets.

ÉTAPE 3 Cliquez sur Submit pour enregistrer les paramètres.

Page Port Status

Utilisez la page Port Status pour activer ou désactiver une interface Ethernet.

ÉTAPE 1 Cliquez sur **Administration > Switch Setting > Port Status**. La fenêtre Port Status s'ouvre.

ÉTAPE 2 Pour activer une interface, cliquez sur **Enabled**. Cette option n'est pas disponible pour les interfaces sans fil ou ADSL.

ÉTAPE 3 Cliquez sur **Submit** pour enregistrer les paramètres.

Page DSL Switch Setting

Utilisez la page DSL Switch Setting pour activer le commutateur DSL sur une interface.

ÉTAPE 1 Cliquez sur **Administration > Switch Setting > DSL Switch Setting**. La fenêtre DSL Switch Setting s'ouvre.

ÉTAPE 2 Pour désactiver l'interface ADSL et convertir le port LAN 4 en mode réseau WAN, cliquez sur **Disabled**.

ÉTAPE 3 Cliquez sur **Submit** pour enregistrer les paramètres.

Page MAC Filtering (modèles SRP540 uniquement)

Vous pouvez contrôler l'accès à votre réseau en indiquant les adresses MAC des périphériques qui ont un accès autorisé ou bloqué.

REMARQUE Seules les interfaces Ethernet filaires prennent en charge le filtrage MAC. Reportez-vous au filtre MAC sans fil pour contrôler l'accès WiFi.

ÉTAPE 1 Cliquez sur **Administration > Switch Setting > MAC Filter**. La fenêtre MAC Filter (Allowed list) s'ouvre.

Cette page permet d'activer le filtrage MAC pour permettre l'accès réseau au modèle SRP et l'affichage de toutes les adresses MAC attribuées aux ports LAN 1-4. Vous pouvez également activer une adresse MAC (si désactivée) et ajouter une entrée d'adresse MAC qui permet d'établir le trafic.

ÉTAPE 2 Pour ajouter une adresse MAC, choisissez le port LAN dans la liste déroulante, saisissez l'adresse MAC correspondante, puis cliquez sur le bouton **Add**.

ÉTAPE 3 Sélectionnez l'option **Enabled** pour activer le filtrage MAC pour les ports LAN 1-4.

ÉTAPE 4 Cliquez sur **Submit** pour enregistrer les modifications.

Status

Utilisez la page Status pour afficher l'état du système et de la mémoire du modèle SRP. Les informations d'état s'affichent en temps réel.

Pour accéder à cette page, cliquez sur **Administration > Status**.

Cette page vous permet d'afficher ce qui suit :

- **CPU**–MIBS, Loads et Uptime.
- **Memory**–Memory's Total size (KB), Free size (%), Used size (%), Buffer size (%), Cached size (%), Active size (%) et Inactive size(%).

9

Utilisation des diagnostics de plates-formes prête pour les services

Ce chapitre décrit comment utiliser les fonctionnalités de diagnostic des plates-formes prêtes pour les services. Il comprend les sections suivantes :

- **Page Ping Test**
- **Page Traceroute**
- **Page Detect Active LAN Client**
- **Page TCP Dump**
- **Page ATM Ping OAM**

Pour accéder à ces pages, cliquez sur **Diagnostics** dans la barre de menu de l'utilitaire de configuration.

Page Ping Test

Utilisez la page Ping Test pour tester la connectivité entre le SRP et un périphérique connecté sur le réseau.

ÉTAPE 1 Cliquez sur **Diagnostics > Ping Test**. La fenêtre Ping Test s'ouvre.

ÉTAPE 2 Saisissez l'adresse IP ou le nom de domaine complet que vous souhaitez tester.

ÉTAPE 3 Saisissez une taille de paquet en octets. La plage est comprise entre 32 et 65 500 octets.

ÉTAPE 4 Choisissez le nombre de tests ping dans la liste déroulante (**5**, **10** ou **Unlimited** (Illimité)).

ÉTAPE 5 Cliquez sur le bouton **Start to Ping** pour lancer le test. Une fois le test terminé, les résultats s'affichent sur la page.

ÉTAPE 6 Pour revenir à la fenêtre précédent, cliquez sur **Close**.

Page Traceroute

Utilisez la page Traceroute pour afficher le routage entre le SRP et une destination.

ÉTAPE 1 Cliquez sur **Diagnostics > Traceroute Test**. La fenêtre Traceroute Test s'ouvre.

ÉTAPE 2 Entrez l'adresse IP ou le nom de domaine complet pour le traçage.

ÉTAPE 3 Cliquez sur le bouton **Start to Traceroute** pour lancer le test. Les résultats s'affichent sur la page et sont actualisés toutes les 5 secondes.

ÉTAPE 4 Pour revenir à la fenêtre précédent, cliquez sur **Close**.

Page Detect Active LAN Client

Utilisez la page Detect Active LAN Client(s) pour détecter les périphériques client actifs sur les réseaux SRP.

ÉTAPE 1 Cliquez sur **Diagnostics > Detect Active LAN Client(s)**. La fenêtre Detect Active LAN Client(s) s'ouvre.

ÉTAPE 2 Choisissez l'interface LAN que vous souhaitez détecter dans la liste déroulante. Par exemple : VLAN1.

ÉTAPE 3 Choisissez la durée pendant laquelle vous souhaitez effectuer cette recherche (**5**, **10** ou **15** secondes).

ÉTAPE 4 Cliquez sur le bouton **Start to Search** pour lancer le test. Une nouvelle fenêtre contenant les résultats du test s'affiche.

ÉTAPE 5 Pour exécuter l'analyse de nouveau, cliquez sur le bouton **Retry**. Pour revenir à la fenêtre précédent, cliquez sur **Close**.

Page TCP Dump

Utilisez la page TCP Dump pour saisir les paquets sur une interface à l'aide de la commande tcpdump.

Le dégagement TCP peut être utilisé pour capturer une partie ou l'intégralité des paquets reçus par une interface réseau. Les paquets saisis sont stockés dans un fichier pcap sur un périphérique de stockage USB relié. Depuis cette page, le fichier peut être téléchargé via l'interface SRP ou utilisé via le périphérique de stockage pour une analyse à l'aide d'une application telle que Wireshark.

REMARQUE Vous pouvez exécuter la commande tcpdump avec « no option » afin de capturer le flux de paquets dans toutes les interfaces. Spécifiez l'option -i pour filtrer une interface Ethernet spécifique. Par exemple : # tcpdump -i eth1.

ÉTAPE 1 Branchez le périphérique USB au port USB spécifié sur le SRP. Pour les emplacements de port USB, reportez-vous au chapitre **Présentation du produit, page 13**.

ÉTAPE 2 Cliquez sur **Diagnostics > TCP Dump**. La fenêtre TCP dump s'ouvre.

ÉTAPE 3 Sélectionnez un périphérique de stockage USB externe dans la liste déroulante. C'est là que le fichier de paquets sera enregistré. Sélectionnez **USB Stick 1** ou **USB Stick 2**. Ces options correspondent aux périphériques USB connectés aux ports USB sur le SRP.

ÉTAPE 4 Choisissez l'interface à utiliser pour capturer les paquets dans la liste déroulante.

ÉTAPE 5 Modifiez le nom de fichier -w si nécessaire. Par exemple : tcpdump.pcap.

ÉTAPE 6 Entrez le temps d'exécution **Run Time** (en secondes) pour exécuter tcpdump. La plage est comprise entre 0 et 86400 secondes. La valeur par défaut est 60 secondes. Tapez 0 pour exécuter la trace indéfiniment. Si vous utilisez cette option, vous devez arrêter manuellement la trace en cas de besoin.

ÉTAPE 7 Si nécessaire, ajustez l'entrée **Advanced Command String** de façon à régler tcpdump via des options de commande standard. Par exemple : -i br0 -w /home/usb_storage_1/tcpdump.pcap.

> **REMARQUE** Par défaut, le SRP capture uniquement les 60 premiers octets de chaque paquet. Si vous désirez davantage de détails, ajoutez « -s 0 » pour retirer cette limite. Les performances du SRP peuvent diminer si le taux de capture du trafic est très élevé. Pour plus d'informations sur les options de dégagement TCP, consultez : http://www.tcpdump.org/tcpdump_man.html.

ÉTAPE 8 Cliquez sur le bouton **Start** pour exécuter le daemon TCP Dump. Cliquez sur le bouton Stop pour l'arrêter. Pour enregistrer le fichier, cliquez sur le bouton **Download dump file to PC.**

Page ATM Ping OAM

Utilisez la page ATM Ping pour envoyer un paquet Operation, Administration and Maintenance (OAM) afin de confirmer la connectivité d'un circuit virtuel permanent (PVC) et de faciliter le dépannage du réseau ATM.

ÉTAPE 1 Cliquez sur **Diagnostics > ATM OAM Ping**. La fenêtre ATM OAM s'ouvre.

ÉTAPE 2 Choisissez l'interface WAN que vous souhaitez tester dans la liste déroulante. Par exemple : PVC0.

ÉTAPE 3 Choisiez le type d'OAM (**F4 End Loopback**, **F4 Segment Loopback**, **F5 End Loopback** ou **F5 Segment Loopback**) dans la liste déroulante.

ÉTAPE 4 Cliquez sur le bouton **Start to Ping** pour lancer le test. Une nouvelle fenêtre contenant les résultats du test s'affiche.

ÉTAPE 5 Pour revenir à la fenêtre précédent, cliquez sur **Close**.

10

Affichage de l'état des plate-formes prêtes pour les services

Ce chapitre décrit comment afficher l'état des plates-formes prêtes pour les services à partir de l'utilitaire de configuration. Il comprend les sections suivantes :

- Page Router Status
- Page Firewall Status
- Page Interface Information
- Page Port Statistics
- Page Wireless Network Status
- Page Wireless Client Information
- Page Guest Network Information
- Page Mobile Network Status
- Page DHCP Pool Information
- Page QoS Status
- Page Routing Table
- Page ARP Table
- Page RIP Status
- Pager IGMP Status
- Page VPN Status
- Page VPN Server Status
- Page CDP Neighbor Information
- Page Status ADSL
- Page STP Status

Pour accéder à ces pages, cliquez sur **Status** dans la barre de menus de l'utilitaire de configuration.

Page Router Status

Utilisez la page **Status > Router** pour afficher des informations sur la SRP et sur l'état de son microprogramme.

État du routeur

Model	Nom et fonctionnalités du produit.
Version ID	Identifiant de la version du produit.
Hardware Version	Numéro de version matérielle.
Boot Version	Numéro de version du microprogramme d'amorçage.
Firmware Version	Version actuelle du microprogramme.
ADSL Firmware Version	Version actuelle du microprogramme ADSL.
Recovery Firmware	Numéro de version du microprogramme de récupération.
Setup Wizard Version	Numéro de version de l'assistant de configuration.
WAN MAC Address	Adresse MAC de l'interface WAN.
Current Time	Heure à laquelle la page a été chargée ; la page ne se met pas à jour.
Wireless	Nombre de SSID sans fil qui sont activés.

Page Firewall Status

Utilisez la page **Status > Firewall** pour afficher les informations sur le pare-feu de la SRP.

État du pare-feu

Stratégie d'accès à Internet	
No	Numéro d'index de la liste de stratégies d'accès à Internet.
Policy Name	Nom de la stratégie d'accès à Internet.

État du pare-feu

Status	État de la stratégie d'accès à Internet. Cliquez sur le lien pour accéder à la configuration des stratégies.
Passed (pkts)	Nombre de paquets transmis par cette règle.
Passed (bytes)	Volume du trafic passé par cette règle, en octets.
Blocked (pkts)	Nombre de paquets bloqués par cette règle.
Blocked (bytes)	Volume du trafic bloqué par cette règle, en octets.
Port Forwarding	État des règles de transfert de port actuellement actives. Les règles qui ne sont pas activées ou qui sont associées à des interfaces WAN déconnectées ne sont pas affichées.
Type	Indique le transfert de port unique ou de plage de ports.
Protocol	Port en cours de transfert.
Port	Port en cours de transfert.
Host	Adresse IP de l'hôte LAN vers lequel effectuer le transfert.
Packets	Nombre de paquets transférés.
Traffic (bytes)	Volume du trafic transféré, en octets.
Statistics	Mesures générales du trafic via le pare-feu.
Name	Nom de la table IP associée au traitement des paquets du pare-feu. **INPUT** : trafic destiné à la SRP. **OUTPUT** : trafic provenant de la SRP. **FORWARD** : trafic transmis entre les réseaux public/externe et privé/interne.
Accept PKT	Nombre de paquets acceptés par ce chemin du pare-feu.
Accept Volume (bytes)	Volume du trafic, en octets, traité par ce chemin du pare-feu.
Drop PKT	Nombre de paquets filtrés/bloqués par ce chemin du pare-feu.
Drop Volume (bytes)	Volume du trafic, en octets, filtré/bloqué par ce chemin du pare-feu.

Page Interface Information

Utilisez la page d'informations **Status > Interface** pour afficher les informations relatives aux différentes interfaces.

REMARQUE Pour afficher des informations supplémentaires sur l'état, cliquez sur un élément de la liste WAN. Le détail de la table d'interface affiche les informations de WAN pour l'interface sélectionnée.

Informations sur l'interface

Liste des interfaces	
Interface	Affiche toutes les interfaces (IP) à trois couches LAN et WAN configurées. Une interface WAN Ethernet est affichée en tant que « Ether_WAN » et une interface WAN ADSL est affichée en tant que « ADSL_PVC ». La numérotation des interfaces est déterminée comme suit : ▪ **Interfaces principales** : la numérotation suit l'étiquetage des ports physiques (c'est-à-dire, WAN1 et WAN2). ▪ **Sous-interfaces WAN Ethernet** : la numérotation reflète l'index VLAN configuré. ▪ **PVC ADSL** : numérotés en série de 0 à 3. ▪ **Interfaces VLAN** : la numérotation reflète l'index VLAN configuré.
Connect Type	Protocole utilisé par l'interface.
IP Address	Adresse IP de l'interface.
Subnet Mask	Masque de sous-réseau de l'interface.
MAC Address	Adresse MAC de l'interface.
Disconnect button	Cliquez sur ce bouton pour déconnecter l'interface, si celle-ci est un tunnel VPN.
Liste des ports	
Interface	Répertorie toutes les interfaces physiques WAN et LAN actuellement configurées (Ethernet, WiFi SSID, DSL PVC).
TX (pkts)	Nombre de paquets transmis à partir de ce port.

Informations sur l'interface

RX (pkts)	Nombre de paquets reçus par ce port.
Status	État de connectivité du port.
Clear TX & RX button	Réinitialise à 0 le nombre de paquets reçus et transmis.

Page Port Statistics

Utilisez la page **Status > Port Statistics** pour afficher les statistiques relatives à l'activité des ports physiques.

Statistiques des ports

Liste des ports	
Port	Affiche les compteurs MIB actuels d'un port physique unique, Ether_WAN1, 4 ports LAN (port LAN 1, port LAN 2, port LAN 3, port LAN 4), et Ether_WAN2.
Columns	▪ **Port** : port physique. ▪ **Input Bytes** : nombre d'octets reçus par le port. ▪ **Output Bytes** : nombre d'octets transmis par le port. ▪ **Input Errors** : nombre d'erreurs de réception détectées pour le trafic entrant. ▪ **Input Broadcasts** : nombre de messages de diffusion Ethernet reçus par l'interface. ▪ **Output Broadcasts** : nombre de messages de diffusion Ethernet envoyés par l'interface. ▪ **Input Multicasts** : nombre de messages de multidiffusion Ethernet reçus par l'interface. ▪ **Output Multicasts** : nombre de messages de multidiffusion Ethernet envoyés par l'interface.

Page Wireless Network Status

Utilisez la page **Status > Wireless Network** pour afficher les informations sur l'état de vos réseaux sans fil.

État du réseau sans fil

Network Mode	Mode de fonctionnement configuré pour le point d'accès sans fil intégré. Pour de plus amples informations, reportez-vous à la section **Configuration d'un LAN sans fil, page 64.**
Radio Band	Bande passante du canal utilisée par le réseau sans fil.
Channel	Canal sans fil actuellement utilisé.
Wireless List	Configuration SSID actuelle. Les colonnes de la liste sans fil incluent : ▪ **SSID Name :** nom SSID configuré. ▪ **Status** : SSID activé ou désactivé. ▪ **Broadcast** : diffusion SSID activée ou désactivée. ▪ **Security** : paramètres de sécurité actuels. ▪ **WPS :** indique si le WPS est activé pour ce SSID.

Page Wireless Client Information

Utilisez la page **Status > Wireless Client** information pour afficher les informations sur les clients sans fil connectés par un SSID.

.

Informations sur le client sans fil

MAC Address	Adresse MAC du client.
Tx-Rate	Débit de données de transmission actuel du client.
Rx-Rate	Débit de données de réception actuel du client.
RSSI	Puissance du signal du dernier paquet reçu.
IDLE	Paramètre actuel du minuteur d'inactivité de la station. Il s'agit du temps, en millisecondes, pendant lequel la station entre en économie d'énergie si aucune activité ne se produit sur le lien.

Page Guest Network Information

Utilisez la page **Status > Guest Network** pour afficher les informations relatives à un client de réseau invité.

État de la liste d'utilisateurs du réseau invité

Account	Nom authentifié de l'utilisateur.
IP Address	Adresse IP DHCP du réseau affectée à l'utilisateur.
MAC	Adresse MAC de la carte réseau de l'utilisateur.
Remain Lease Time	Temps restant disponible avant la fin de session utilisateur.
Disconnect	Cliquez sur ce bouton pour mettre fin à une session.

Page Mobile Network Status

Utilisez la page **Status > Mobile Network Status** pour afficher les informations relatives au modem haut débit USB qui est installé sur la SRP.

REMARQUE Cette page varie selon le type de modem USB que vous avez installé.

État du modem du réseau mobile

Connection	Affiche l'état du modem : Connected ou Unable to Detect USB Mobile Modem (indique si aucun modem n'est installé).
Internet IP Address	Adresse IP attribuée au modem USB.
Subnet Mask	Masque de sous-réseau du réseau mobile.
Default Gateway	Adresse IP de la passerelle attribuée par le FAI.
DNS	Adresse IP du serveur DNS attribuée par le FAI.
Connection Up Time	Durée de la session de connexion actuelle.
Current Session Usage	Volume du trafic reçu et émis.

État du modem du réseau mobile

État de la carte de données	
Manufacturer	Fabricant du modem USB connecté.
Card Model	Nom de modèle du modem USB connecté.
Card Firmware	Révision du microprogramme actuellement installée sur le modem USB.
SIM Status	État de la carte SIM (compatible SIM ou code PIN requis).
IMSI	Numéro d'identification internationale d'abonné mobile (IMSI) de ce modem USB. Il s'agit d'un numéro unique stocké dans le SIM (Subscriber Identity Module), associé à tous les utilisateurs de téléphones mobiles des réseaux GSM et UMTS (système universel de télécommunications mobiles).
Carrier	Fournisseur de service réseau utilisé pour la connexion Internet.
Service Type	Type de service de modem USB.
Signal Strength	Puissance du signal du service UMTS/GPRS/EVDO actuel.
Card Status	État de la carte : Connecting, Connected, Disconnecting, Disconnected ou Card is not activated. Si aucune carte n'est connectée, la page d'état indique le message suivant concernant le SRP : « Unable to Detect USB Mobile Modem ».

Paramètres de la carte USB CDMA2000 EVDO

Connection	Affiche l'état du modem. Connected ou Unable to Detect USB Mobile Modem (s'affiche si aucun modem n'est installé).
IP Address	Adresse IP attribuée au modem USB.
Connection Up Time	Durée de la session de connexion actuelle.
Current Session Usage	Volume du trafic reçu et émis.
Manufacturer	Fabricant du modem USB connecté.

Paramètres de la carte USB CDMA2000 EVDO

Card Model	Nom de modèle du modem USB connecté.
Card Firmware	Révision du microprogramme actuellement installée sur le modem USB.
ESN	Numéro de série électronique (ESN) de ce modem USB.
PRL Version	Version PRL de ce modem USB.
Phone Number	Numéro de téléphone associé au compte de ce modem USB.
Carrier	Nom de l'opérateur associé au service de modem USB.
Signal Strength	Puissance du signal.
Card Status	État de la carte : Connecting, Connected, Disconnecting, Disconnected ou Card is not activated. Si aucune carte n'est connectée, la page d'état indique le message suivant concernant le SRP : « Unable to Detect USB Mobile Modem ».

Page DHCP Pool Information

Utilisez la page **Status > DHCP Pool Information** pour afficher les informations sur le bail du serveur DHCP par règle.

Informations sur le pool DHCP

Client Name	Nom d'hôte du client DHCP.
IP Address	Adresse IP louée au client.
MAC Address	Adresse MAC du client DHCP.
Expires Time	Date d'expiration du bail DHCP actuel.
Interface	Interface via laquelle le client est connecté.

Page QoS Status

Utilisez la page **Status > QoS** pour afficher les statistiques de mise en file d'attente du trafic. La SRP prend en charge 5 files d'attente : une file d'attente stricte et quatre files d'attente « Round Robin » pondérées.

REMARQUE Pour afficher cette page, vous devez activer l'une des interfaces à partir de la page **Network Setup > QoS > QoS Bandwidth Control**. Voir aussi **Page QoS Bandwidth Control, page 92.**

État QoS

Queue Name	Répertorie les cinq files d'attente utilisées par la SRP (Strict High, High, Medium, Normal et Low).
Config Rate	Quantité nominale de trafic que chaque file d'attente peut prendre en charge dans des conditions équilibrées et chargées. La bande passante non utilisée par une file d'attente peut être utilisée par une autre, ce qui implique que la bande passante de mise en file d'attente configurée peut être dépassée.

État QoS

Allow Maximum Rate	Débit du trafic maximal autorisé, en Kbits/s, pour chaque file d'attente. Cela permet aux files d'attente « Round Robin » pondérées d'utiliser toutes les bandes passantes formées, alors que le trafic de file d'attente hiérarchisée est limité à 70 % du total pour garantir la prise en charge fiable du contenu multimédia en temps réel.
Send (bytes)	Nombre d'octets envoyés à partir de cette file d'attente.
Send (pkts)	Nombre de paquets envoyés à partir de cette file d'attente.
Drop	Nombre de paquets abandonnés lorsque le débit total du trafic dépasse le débit maximal autorisé.
Overlimits	Nombre de paquets qui ont été abandonnés lorsque le débit du trafic est supérieur au débit maximal autorisé.
Requeues	Si un paquet ne peut pas être envoyé, il est remis dans la file d'attente d'origine pour une autre tentative. Cet événement augmente le compteur de remises dans la file d'attente.
Current Rate (bps)	Débit actuel pour cette file d'attente, en bits par seconde.

Page Routing Table

Utilisez la page **Status > Routing Table** pour afficher les informations sur le routage.

État de la table de routage

Destination LAN IP	Adresse du réseau ou de l'hôte auquel l'itinéraire statique est attribué.
Subnet Mask	Indique quelle partie d'une adresse IP correspond à la partie réseau et quelle partie correspond à la partie hôte.
Gateway	Adresse IP du périphérique passerelle qui permet le contact entre la passerelle et le réseau ou l'hôte.

État de la table de routage

Interface	Indique si l'adresse IP de destination se trouve sur le LAN et sur un réseau sans fil (réseaux filaires et sans fil internes) ou sur Internet (WAN).

Page ARP Table

Utilisez la page **Status > ARP Table** pour afficher les informations sur tout l'ARP (Address Resolution Protocol, protocole de résolution d'adresse).

État de la table ARP

Adresse IP	Adresse IP du périphérique.
HW Address	Adresse MAC du périphérique.
Périphérique	Interface via laquelle l'adresse a été obtenue.

Page RIP Status

Utilisez la page **Status > RIP** pour afficher les informations sur toutes les activités RIP (protocole Routing Information Protocol). Cette page sauvegarde tous les messages RIP relatifs au daemon RIP associé. Pour chaque itinéraire reçu via le RIP, elle affiche l'heure d'envoi du paquet et les informations sur les balises. Elle affiche également l'état du RIP actuel, tel que le minuteur RIP, le filtrage, la version, l'interface activée par RIP et les informations sur les homologues du RIP.

Pager IGMP Status

Utilisez la page **Status > IGMP Status** pour afficher les informations IGMP (Internet Group Management Protocol).

IGMP Status

IP Address	Groupe de multidiffusion que les clients LAN ont rejoint.
Port	Répertorie les ports connectés au groupe d'adresse de multidiffusion.

Page VPN Status

Utilisez la page **Status > VPN Status** pour afficher les informations sur l'état du VPN.

État du VPN

Tunnel Name	Nom du tunnel VPN.
Remote Policy	Stratégie réseau distant.
Local Policy	Stratégie réseau local.
IKE Algorithm	Résultat final de l'algorithme IKE après ISAKMP. Concerne uniquement le mode « AUTO ».
IPSec Algorithm	Algorithme IPSec que ce tunnel utilise actuellement.
TX Bytes	Nombre d'octets transmis à partir de ce tunnel.
RX Bytes	Nombre d'octets reçus de ce tunnel.
Connect Status	Concerne uniquement le mode « AUTO ».

Page VPN Server Status

Utilisez la page **Status > VPN Server Status** pour afficher les informations relatives aux clients VPN IPSec connectés au serveur VPN. Le serveur VPN peut prendre en charge jusqu'à 5 connexions de clients VPN sur les modèles SRP520 et jusqu'à 10 sur les modèles SRP540.

VPN Server Status

WAN IP Address	Adresse IP utilisée par le client VPN pour établir un tunnel avec le serveur VPN.
IP Address	Adresse IP attribuée par le serveur VPN. Cette adresse est spécifiée sur la page **VPN > Cisco VPN Server > Group**, sous Mode Configuration.
XAUTH Name	Nom du compte utilisé par le client VPN pour authentifier le serveur VPN qui utilise la méthode PSK+XAUTH. **REMARQUE** Si le serveur VPN utilise uniquement l'authentification « PSK », ce champ affiche un symbole « -- » qui indique que XAUTH n'est pas utilisé.

Page CDP Neighbor Information

Utilisez la page **Status > CDP Neighbor Information** pour afficher les informations sur le voisinage du CDP.

Informations sur le voisinage du CDP

Informations sur le voisinage	
Device ID	Numéro d'identifiant du périphérique voisin.
Local Interface	L'interface SRP à laquelle le voisin du CDP est connecté.
Hold Time	Temps d'attente avant le rejet de paquets par le CDP.
Capability	Classe du voisin.
IP Address	10.52.204.254

Pour afficher des informations supplémentaires sur l'état, cliquez sur un élément de la liste Neighbor information. La table CDP Details affiche les informations relatives au périphérique sélectionné.
Par exemple :

```
Name: Value
Device ID: SBTG-4948
Local Interface: LAN Port 1
Hold Time: 30 sec.
Capability: R, S, I
```

```
Platform: cisco WS-C4948
Port ID: GigabitEthernet1/31
IP address: 10.52.204.254
```

Page Status ADSL

Utilisez la page **Status > ADSL Status** pour afficher les paramètres d'état du PVC et de l'ADSL de la SRP.

Page ADSL Status

Cette page affiche des informations ADSL sur la SRP. Ces informations varient selon le type de connexion Internet spécifié sur la page **Internet Setup > WAN > Internet Setup**.

Paramètres d'état de l'ADSL

DSL Status	État de la ligne DSL actuelle. Les états possibles sont : ▪ **Idle** : la ligne est déconnectée. ▪ **G.994 training** : le modem se forme au service DSL. ▪ **G.992 Started** : un service ADSL a été détecté et le service est en cours de démarrage. ▪ **G.922 Channel Analysis** : le modem évalue l'utilisation du canal DSL. ▪ **G.992 Message Exchange** : le modem établit une connexion ADSL. ▪ **Showtime** : l'apprentissage du modem ADSL s'est effectué avec succès et ce dernier fonctionne normalement.
DSL Modulation Mode	Mode de modulation actuellement utilisé par le modem ADSL.

Paramètres d'état de l'ADSL

Downstream Rate	débit de données en aval actuel, en Kbits/s. Ce chiffre indique le débit maximal du circuit virtuel permanent (PVC) ADSL. Dans la pratique, l'encombrement du réseau ou les stratégies de débit imposées par votre prestataire de services peuvent entraîner des taux inférieurs.
Upstream Rate	débit de données en amont actuel, en Kbits/s. Ce chiffre indique le débit maximal de la connexion ADSL. Dans la pratique, l'encombrement du réseau ou les stratégies de débit imposées par votre prestataire de services peuvent entraîner des taux inférieurs.
Downstream Noise Margin	Marge de bruit en aval/Rapport signal/bruit en dB.
Upstream Noise Margin	Marge de bruit en amont mesurée/Rapport signal/bruit, en dB.
Downstream Line Attenuation	Atténuation de ligne en aval, en dB.
Upstream Line Attenuation	Atténuation de ligne en amont, en dB.
Downstream Transmit Power	Puissance de transmission en aval, en dBm.
Upstream Transmit Power	Puissance de transmission en amont, en dBm.

Page PVC Status

Utilisez la page **Status > PVC Status** pour afficher les informations de connectivité relatives à chacun des PVC configurés sur l'interface DSL.

État du PVC

Interface	Nom de l'interface PVC.
Interface	Type d'encapsulation configuré pour le PVC.
VPI	Identificateur de chemin virtuel du PVC. Cette valeur peut être configurée manuellement ou automatiquement détectée.

État du PVC

VCI	Identificateur de circuit virtuel du PVC. La valeur peut être configurée manuellement ou automatiquement détectée.
PVC Status	État de la configuration actuelle du PVC (appliqué).

Page STP Status

Utilisez la page **Status > STP** pour afficher les informations sur toutes les activités STP (protocole Spanning Tree Protocol). Cette page sauvegarde tous les messages STP relatif au daemon STP associé et affiche les informations d'état, telles que les informations sur le pontage, le retard de transfert, le paquet Hello et la durée d'attente.

A

Spécifications

Cette annexe présente les spécifications des plates-formes prêtes pour les services.

Caractéristiques SRP520-U

Fonctionnalité	Modèle
WAN	▪ SRP521W-U : Commutateurs ▪ SRP526W-U : ADSL2+ (Annexe B) ▪ SRP527W-U : ADSL2+ (Annexe A)
LAN	4 ports Fast Ethernet
Sans fil	Point d'accès 802.11b/g/n avec antenne captive unique
Ports voix	2 ports de téléphone (FXS), 1 port de ligne (FXO) utilisé pour le mode de relais de ligne de secours uniquement
Ports USB	1 port USB 2.0
Température de fonctionnement	-32° F à 140° F (0° C à 40° C)
Température hors fonctionnement	-22° F à 158° F (-30° C à 70° C)
Humidité de fonctionnement	de 5 à 95 % (sans condensation)
Gamme de tensions	100-240V 50/60 Hz CA
Dimensions	(L x P x H) : 170 mm (6,69 pouces) x 170 mm (6,69 pouces) x 42 mm (1,65 pouces)
Poids	400 g (0,89 livres).

Caractéristiques SRP540

Fonctionnalité	Modèle
WAN	▪ SRP541W : 2 ports WAN Gigabit Ethernet ▪ SRP546W : ADSL2+ Annexe B (ADSL sur ISDN)/1 port WAN Gigabit Ethernet ▪ SRP547W : ADSL2+ Annexe A/M (ADSL sur POTS) /1 port WAN Gigabit Ethernet
LAN	4 ports LAN Gigabit Ethernet
Sans fil	Point d'accès 802.11b/g/n avec deux antennes amovibles (TNC)
Ports voix	4 ports téléphoniques (FXS), 1 port de ligne (FXO)
Ports USB	2 ports USB 2.0
Température de fonctionnement	-32° F à 140° F (0° C à 40° C)
Température hors fonctionnement	-22° F à 158° F (-30° C à 70° C)
Humidité de fonctionnement	de 5 à 95 % (sans condensation)
Gamme de tensions	100-240V 50/60 Hz CA
Dimensions	(L x P x H) : 220 mm (8,66 pouces) x 170 mm (6,69 pouces) x 44 mm (1,73 pouces)
Poids	▪ SRP541W : 930g (2,05 livres). ▪ SRP546W/SRP547W : 962 g (2,12 livres).

B

Pour en savoir plus

Cisco propose une vaste gamme de ressources pour vous aider, ainsi que vos client,s à tirer pleinement parti des plateformes prêtes pour les services.

Ressources sur les produits

Prise en charge	
Communauté d'assistance Cisco Small Business	www.cisco.com/go/smallbizsupport Pour obtenir plus d'informations sur la SRP, cliquez sur Small Business Routers dans la page Community.
Assistance technique et documentation en ligne (identification obligatoire)	www.cisco.com/support
Ressources et assistance Cisco Small Business	www.cisco.com/go/smallbizhelp
Coordonnées de l'assistance téléphonique	www.cisco.com/go/sbsc
Logiciels	
Téléchargement de logiciels (identifiant de connexion obligatoire)	www.cisco.com/go/srp500 Cliquez sur le lien Download Software.
Documentation Open Source	www.cisco.com/en/US/products/ps10500/prod_release_notes_list.html
Documentation sur les produits	
Plateforme prête pour les services de la gamme Cisco 500 pour les petites entreprises	www.cisco.com/go/srp500resources

Cisco Small Business	
Partenaires et revendeurs Cisco pour les PME (identification partenaire obligatoire)	www.cisco.com/web/partners/sell/smb
Accueil Cisco Small Business	www.cisco.com/smb
Marketplace	www.cisco.com/go/marketplace