



GUIDE D'ADMINISTRATION

**Plates-formes prêtes pour les services de la
gamme Cisco SRP500 (Modèles SRP520)**

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. L'utilisation du terme « partenaire » n'implique pas de relation de partenariat entre Cisco et toute autre entreprise. (1005R)

Chapitre 1 : Présentation des plates-formes prêtes pour les services de la gamme SRP500 (modèles SRP520)	10
Présentation des caractéristiques	10
Présentation du produit	11
Numéros de modèle	11
Façade avant	12
Façade du modèle SRP521W	12
Façade avant SRP526W/SRP527W	12
Voyants de la façade	12
Panneau arrière	13
Panneau arrière du modèle SRP521W	13
Façade arrière SRP526W/SRP527W	14
Description du panneau arrière	14
Vue latérale	15
Vue du dessus	16
Paramètres par défaut	17
Chapitre 2 : Mise en route à l'aide de l'utilitaire de configuration	18
Connexion à l'utilitaire de configuration	18
Présentation de l'utilitaire de configuration	19
Zones de la fenêtre principale	19
Icônes de l'utilitaire de configuration	20
Chapitre 3 : Le menu Quick Setup	21
Installation de la configuration de base	21
Page WAN Setup(Ethernet)	21
Page WAN Setup (ADSL)	26
Page LAN Setup	28
Page Wireless Setup	30
Page Remote Provisioning	35
Configuration avancée	37
Option Voice	37
Option Mobile Network Setup	37

Option Firewall	37
Option NAT	37

Chapitre 4 : Configuration des interfaces des plates-formes prêtes pour les services 38

Configuration de l'interface WAN	38
Page Internet Setup	39
Paramètres VC	41
Paramètres IPOA / Static IP	41
Paramètres PPPoE	42
Paramètres PPPoA	43
Page Mobile Network	44
Page Failover & Recovery (SRP521W)	48
Page Failover & Recovery (SRP526W, SRP527W)	50
Configuration des interfaces VLAN et des ports WAN	52
Page DHCP Server	52
Page VLAN Setting	55
Page Port Settings	57
Configuration du LAN sans fil	58
Page Basic Wireless Settings	59
Page Wi-Fi Protected Setup	68
Méthode WPS 1	68
Méthode WPS 2	68
Méthode WPS 3	69
Page Wireless MAC	69
Page Advanced Wireless Settings	71
Page WMM Setting	74
Utilisation de l'interface de gestion	75

Chapitre 5 : Configuration du réseau 76

Page Routing	77
Page Static Routes	77
Page RIP	78
Page Intervlan Routing	80

Page NAT	80
Page NAT Setting	80
Page Port Forwarding	81
Page Port Range Triggering	83
Page QoS	85
Page QoS Bandwidth Control	85
Page QoS Policy	86
Page CoS To Queue	88
Page DSCP To Queue	89
Page Firewall	89
Page Firewall Filter	90
Page Internet Access Control	92
Page PPPoE Relay	94
Page DDNS	96
Page DMZ	98
Page IGMP	99
Page UPnP	100
Page CDP Setting	101

Chapitre 6 : Configuration de la voix 103

Configuration des Services Voix	103
Opérations de compréhension des ports voix	103
Fonctionnalités voix du SRP	104
Codecs pris en charge	105
Redondance du proxy SIP	105
Autres fonctionnalités voix du SRP	106
Enregistrement auprès du prestataire de services.	112
Gestion des services d'ID de l'appelant	114
Optimisation des taux d'aboutissement de la télécopie	116
Résolution des problèmes liés au fax	117
Suppression des silences et services CNG (Comfort Noise Generation)	118
Configuration des plans de numérotation	119

À propos des plans de numérotation	119
Séquences de chiffres	119
Exemples de séquence de chiffres	122
Réception et transmission des chiffres composés	124
Temporisateur du plan de numérotation (temporisateur de décrochage)	125
Syntaxe du temporisateur du plan de numérotation	125
Exemples de temporisateur du plan de numérotation	125
Temporisateur long inter-chiffres (temporisateur de saisie incomplète)	126
Syntaxe du temporisateur long inter-chiffres	126
Exemple de temporisateur long inter-chiffres	126
Temporisateur court inter-chiffres (temporisateur de saisie complète)	127
Syntaxe du temporisateur court inter-chiffres	127
Exemples de temporisateurs court inter-chiffres	127
Modification des plans de numérotation	127
Saisie du plan de numérotation de l'interface de ligne	128
Réinitialisation des temporisateurs de contrôle	128
Implémentation d'appel sécurisé	129
Activation des appels sécurisés	129
Détails des appels sécurisés	130
Utilisation d'un Mini-certificat	131
Génération d'un mini certificat	132
Configuration des paramètres de voix	133
Page Info	133
Page Product Information	133
Page System Status	134
Page Line Status	135
Page System	137
Page System Configuration	137
Page Miscellaneous Settings	137
Page SIP	138
Page SIP Parameters	138
Page SIP Timer Values	141
Page Response Status Code Handling	143
Page RTP Parameters	144
Page SDP Payload Types	146
Page NAT Support Parameters	147
Page Provisioning	150
Page Configuration Profile	150
Page Firmware Upgrade	154

Page General Purpose Parameters	155
Page Regional	156
Définition des scripts de cadence et de tonalité de la sonnerie	156
Page Call ProgressTones	158
Page Distinctive Ring Patterns	161
Page Distinctive Call Waiting Tone Patterns	162
Page Distinctive Ring/CWT Pattern Names	163
Spécification de la tonalité d'appel en attente et de sonnerie	164
Page Control Timer Values (sec)	165
Page Vertical Service Activation Codes	168
Page Vertical Service Announcement Codes	174
Page Outbound Call Codec Selection Codes	174
Page Miscellaneous	175
Pages Line (1-2)	178
Page Line Enable	179
Page Streaming Audio Server (SAS)	179
Page NAT Settings	180
Page Network Settings	181
Page SIP Settings	182
Page Call Feature Settings	186
Page Proxy and Registration	188
Page Subscriber Information	190
Page Supplementary Service Subscription	191
Page Audio Configuration	193
Page Dial Plan	198
FXS Port Polarity Configuration	199
Pages User (1-2)	200
Page Call Forward Settings	200
Page Selective Call Forward Settings	201
Page Speed Dial Settings	201
Page Supplementary Service Settings	202
Page Distinctive Ring Settings	204
Page Ring Settings	204

Chapitre 7 : La configuration VPN 205

Page IKE Policy	205
Page IPSec Policy	207
Page GRE Tunnel	210

Page VPN Passthrough	212
Page Serveur Cisco VPN	213
Page Users	216

Chapitre 8 : Paramètres d'administration 217

Page Web Access Management	217
Page Remote Management	219
TR069	219
SNMP	221
Local TFTP	222
Page Time Setup	223
Assistant de configuration	224
Page User List	225
Page User Privilege Control	225
Page Log	226
Page Factory Defaults	227
Page Firmware Upgrade	227
Page Backup & Restore	228
Page Backup Configuration	228
Page Restore Configuration	228
Page Reboot	229
Page Status	229
Page Switch Setting	230

Chapitre 9 : Utilisation des diagnostics de la plateforme prête pour les services 231

Page Ping Test	231
Page Traceroute Test	232
Page Detect Active LAN Clients	232

Chapitre 10 : Affichage de l'état des plate-formes prêtes pour les services	233
Page Router	234
Page Firewall Status	235
Page Interface Information	237
Page Wireless Network Status	238
Page Wireless Client Information	239
Page Mobile Network Status	239
Page DHCP Server Information	241
Page QoS Status	242
Page Routing Table	243
Page ARP Table	243
Page RIP Status	244
Page IGMP Status	244
Page VPN Status	245
Page CDP Neighbor Information	246
 Annexe A : Spécifications	 247
 Annexe B : Pour en savoir plus	 249

Présentation des plates-formes prêtes pour les services de la gamme SRP500 (modèles SRP520)

Merci d'avoir choisi les plates-formes prêtes pour les services de la gamme Cisco SRP500 (modèles SRP520). La gamme SRP500 est constituée de périphériques adaptés 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 :

- **Présentation des caractéristiques**
- **Présentation du produit**

Pour obtenir des informations sur l'installation du SRP et sur l'installation de l'assistant de configuration pour sa configuration initiale, reportez-vous au Guide de démarrage rapide des plates-formes prêtes pour les services de la gamme Cisco SRP500 (modèles SRP520) à l'adresse suivante : www.cisco.com/go/srp500/

Présentation des caractéristiques

Merci d'avoir choisi la gamme services Cisco SRP500 de plates-formes prêtes pour les services de (modèles SRP520).

Les plates-formes de la gamme SRP 500 comprennent les fonctionnalités suivantes :

- Intelligence pour la prise en charge des services voix, de données, de sécurité et d'applications.

- Pile de protocole SIP (Session Initiation Protocol) de pointe pour fournir un service voix clair et de grande qualité.
- Interopérabilité avec les commutateurs logiciels courants et les passerelles voix.
- Sécurité intégrée, capacités VPN et un point d'accès sans fil 802.11n.
- Mise en service basée sur des normes pour les déploiements rationalisés.

Présentation du produit

Pour vous aider à vous familiariser avec votre SRP, cette section propose une description des différents modèles disponibles et présente des schémas de la façade avant, de la façade arrière, ainsi que des côtés du système.

Numéros de modèle

Le tableau suivant décrit les références du modèle SRP520 :

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

Façade avant

Façade du modèle SRP521W



Façade avant SRP526W/SRP527W



Voyants de la façade

Le tableau suivant décrit les voyants de la façade de la SRP. Ces voyants permettent de surveiller l'activité du système.

Voyants (verts)	Description
POWER/SYS	S'allume une fois que la SRP a démarré et qu'elle est prête à être utilisée. Clignote pendant le démarrage de la SRP.
Ports LAN (1–4)	S'allume lorsqu'une liaison est établie. Clignote en présence d'activité sur le port LAN.
Port WAN (SRP521W uniquement)	S'allume lorsqu'une liaison est établie. Clignote en présence d'activité sur le port WAN.
Ports téléphoniques (FXS) (1–2)	S'allume lorsqu'une liaison est établie. Clignote en présence d'une activité sur le port téléphonique.

DSL CD	Clignote lorsqu'un service DSL est détecté. Se stabilise au vert une fois la synchronisé.
DSL Data (SRP526W/SRP527W uniquement)	Clignote lorsqu'une activité DSL a lieu sur la ligne.
WLAN	S'allume lorsque le système radio est sous tension et opérationnel. Clignote en présence d'activité sans fil sur le port WLAN.
Port USB	S'allume lorsque le périphérique USB connecté est opérationnel. Clignote en cas de panne ou de non-prise en charge d'un périphérique.
Bouton WPS	S'allume lorsque la fonction WiFi Protected Setup (WPS) est opérationnelle. 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 arrière

Le panneau arrière permet de connecter les périphériques réseau. Les ports situés sur le panneau peuvent varier en fonction du modèle.

Panneau arrière du modèle SRP521W



Façade arrière SRP526W/SRP527W



Description du panneau arrière

Fonctionnalité	Description
Port DSL SRP526/SRP527W uniquement	Permet de raccorder la SRP à la ligne 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 séparée (comme c'est souvent le cas au Royaume-Uni), il se peut que vous deviez brancher un adaptateur spécifique, entre le SRP et votre téléphone, permettant au téléphone d'émettre une sonnerie lorsque des appels se présentent.
Port de ligne (FXO)	Permet de raccorder l'unité au RTPC (Réseau Téléphonique Public Commuté), qui constitue le réseau traditionnel de service téléphonique analogique.
Port WAN (10/100) SRP521W uniquement	Permet de raccorder la SRP au réseau étendu (WAN).
Ports LAN (10/100) (1–4)	Permettent de raccorder l'unité à un ordinateur branché ou à d'autres périphériques réseau.
Interrupteur marche/arrêt	Permet de mettre la SRP sous ou hors tension.
Alimentation 12 VCC	Se branche à l'adaptateur d'alimentation fourni.

Vue latérale



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 d'usine de la SRP. Pour appuyer sur le bouton, insérez un trombone ou tout autre objet similaire dans l'ouverture.
Port USB	Permet de raccorder l'unité à un modem USB compatible. Pour obtenir des informations sur la connexion du SRP à un port USB, reportez-vous à la section Page Mobile Network, page 44 .
Antenne	Antenne Wi-Fi.

Vue du dessus



Fonctionnalités	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

Paramètres	Valeur
Périphérique IP	192.168.15.1
Nom d'utilisateur	cisco
Mot de passe	cisco
Nom d'utilisateur d'administrateur	admin
Mot de passe d'administrateur	admin
Plage DHCP	192.168.15.100 à 149
VLAN de données	VLAN 1
VLAN voix	VLAN 100, publié sur les téléphones Cisco VOIP via CDP

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

Ce chapitre décrit comment configurer et utiliser l'utilitaire de configuration des plate-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'utilitaire de configuration**

Connexion à l'utilitaire de configuration

Cette section décrit comment se connecter à l'utilitaire de configuration des plate-formes prêtes pour les services.

ÉTAPE 1 Connectez un ordinateur au port LAN disponible de votre SRP. Par défaut, votre ordinateur devient un client DHCP de la SRP et reçoit une adresse IP dans la plage 192.168.15.x.

ÉTAPE 2 Ouvrez un navigateur Web.

Dans la barre d'adresse, entrez **http://192.168.15.1**. Il s'agit de l'adresse par défaut de la SRP.

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

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

Le mot de passe par défaut est **admin**.

REMARQUE Les mots de passe sont sensibles à la casse.

REMARQUE Si vous vous connectez en tant que **cisco** (avec le mot de passe **cisco**), l'assistant de configuration s'ouvrira automatiquement. Si vous vous connectez en tant qu'admin, vous pouvez lancer l'assistant de configuration en cliquant sur **Administration > Setup Wizard**.

ÉTAPE 4 Cliquez sur **Log In**. L'utilitaire de configuration des plate-formes prêtes pour les services s'ouvre.

Présentation de l'utilitaire de configuration

Zones de la fenêtre principale

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



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.

Numéro	Composant	Description
2	Volet de navigation	Permet de passer facilement d'une fonctionnalité de périphérique configurable à une autre. Les branches principales se développent pour afficher les fonctionnalités secondaires. Cliquez sur le triangle 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 de l'utilitaire de configuration

L'utilitaire de configuration dispose d'icônes et de boutons pour les options de configuration couramment utilisées. Le tableau suivant décrit ces icônes :

Icône	Description
 Icône Edit	L'icône Edit vous permet de modifier un élément existant à partir d'une liste. Après avoir effectué les modifications souhaitées, cliquez sur le bouton Submit pour enregistrer vos modifications.
 Icône Add Item	L'icône Add Item vous permet d'ajouter un élément à une liste. Après avoir créé un nouvel élément, cliquez sur le bouton Submit pour enregistrer le nouvel élément.
 Icône Delete Item	L'icône Delete Item vous permet de supprimer un élément d'une liste. Après avoir supprimé un élément, cliquez sur le bouton Submit pour enregistrer vos modifications.
 Icônes Increment et Decrement	Les icônes Increment et Decrement vous permettent de modifier les valeurs numériques. Cliquez sur l'icône « + » pour incrémenter une valeur et cliquez sur l'icône « - » pour décrémenter une valeur. Cliquez sur le bouton Submit pour enregistrer vos modifications.

Le menu Quick Setup

Ce chapitre explique comment utiliser le menu Quick Setup pour installer les fonctionnalités de connectivité essentielles pour vos plates-formes prêtes pour les services. Il comprend les sections suivantes :

- **Installation de la configuration de base**
- **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.

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

Installation de la configuration de base

Les fonctionnalités de l'installation de la configuration de base vous permettent d'installer votre mise en service WAN, LAN, sans fil et à distance.

Page WAN Setup(Ethernet)

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

-
- ÉTAPE 1** Cliquez sur **Quick Setup > WAN Setup**. La fenêtre *WAN Setup* s'ouvre.
- ÉTAPE 2** Entrez votre type de connexion Internet et n'importe quel paramètre WAN facultatif, selon les besoins.
- ÉTAPE 3** Cliquez sur **Submit** pour enregistrer les paramètres.
-

Champ	Description
WAN	L'interface WAN.
VLAN ID	L'ID du VLAN.
Connection Type	Le type de connexion Internet que votre ISP fournit à partir du menu déroulant.
	Automatic Configuration - DHCP Par défaut, le type de connexion Internet du routeur est configuré sur Automatic Configuration - DHCP , qui doit être conservé uniquement si votre ISP prend en charge DHCP ou vous vous connectez à l'aide d'une adresse IP dynamique.
	Static IP Si vous devez utiliser une adresse IP permanente pour vous connecter à Internet, sélectionnez Static IP. - Internet IP Address and Subnet Mask Il s'agit de l'adresse IP et du masque de sous-réseau du routeur, tels qu'ils sont visibles par des utilisateurs externes sur Internet (notamment votre ISP). Si votre connexion Internet requiert une adresse IP statique, votre ISP vous fournira une adresse IP statique et un masque de sous-réseau. - Default Gateway Votre ISP vous fournira l'adresse IP de la passerelle. - DNS 1-3 Le système de noms de domaine (DNS) correspond à la manière dont Internet traduit les noms de domaine ou de sites Web en adresses Internet ou URL. Votre ISP vous fournira au moins une adresse IP du serveur DNS. Si vous souhaitez en utiliser une autre, entrez cette adresse IP dans l'un de ces champs. Vous pouvez entrer jusqu'à trois adresses IP du serveur DNS ici. Le routeur utilise ces dernières pour un accès plus rapide aux serveurs DNS en fonctionnement.

Champ	Description
	PPPoE (pour l'utilisateur ADSL) Certains ISP basés sur le DSL utilisent le protocole PPPoE (Point-to-Point Protocol over Ethernet) pour établir des connexions Internet. Si vous êtes connecté à Internet via une ligne DSL, consultez votre ISP pour savoir s'il utilise ce protocole PPPoE. ▪ User Name and Password Entrez le nom d'utilisateur et le mot de passe que vous utilisez lorsque vous vous connectez à votre ISP via une connexion PPPoE. ▪ Service Name S'il est fourni par votre ISP, entrez le nom du service. ▪ Connect on Demand Vous pouvez configurer le routeur pour déconnecter votre connexion Internet après une période d'inactivité spécifiée (inactivité maximale). Si votre connexion Internet a été interrompue en raison de l'inactivité, Connect on Demand permet au routeur de rétablir automatiquement la connexion dès que vous essayez d'accéder à nouveau à Internet. Si vous souhaitez activer Connect on Demand, cliquez sur le bouton radio. Si vous souhaitez que votre connexion Internet reste active à tout moment. Sinon, entrez le nombre de minutes que vous souhaitez laisser s'écouler avant interruption de votre connexion Internet. ▪ Keep Alive Cette option conserve votre connexion à Internet indéfiniment, même lorsque votre connexion est inactive. Si vous souhaitez sélectionner cette option, cliquez sur le bouton radio Keep Alive. La période de recomposition par défaut est de 30 secondes (en d'autres termes, le routeur vérifiera la connexion Internet toutes les 30 secondes).

Champ	Description
	PPTP Le protocole de tunnellation point à point (PPTP) est un service qui concerne les connexions de tunnellation. ▪ Internet IP Address and Subnet Mask L'adresse IP et le masque de sous-réseau, tels qu'ils sont visibles par les utilisateurs externes sur Internet (notamment votre ISP). Si votre connexion Internet requiert une adresse IP statique, votre ISP vous fournira une adresse IP statique et un masque de sous-réseau. ▪ Gateway Votre ISP vous fournira l'adresse IP de la passerelle. ▪ DNS 1-3 Votre ISP vous fournira au moins une adresse IP du serveur DNS. Si vous souhaitez en utiliser une autre, entrez cette adresse IP dans l'un de ces champs. Vous pouvez entrer jusqu'à trois adresses IP du serveur DNS ici. Le routeur utilise ces dernières pour un accès plus rapide aux serveurs DNS en fonctionnement. ▪ PPTP Server IP Il s'agit de l'adresse IP du serveur PPTP. Entrez l'adresse IP qui vous a été communiquée par votre ISP. ▪ User Name and Password Entrez le nom d'utilisateur et le mot de passe que vous utilisez lorsque vous vous connectez à votre ISP via une connexion PPTP. ▪ Connect on Demand Si votre connexion Internet a été interrompue en raison de l'inactivité, Connect on Demand permet au routeur de rétablir automatiquement la connexion dès que vous essayez d'accéder à nouveau à Internet. Si vous souhaitez activer Connect on Demand, cliquez sur le bouton radio. Si vous souhaitez que votre connexion Internet reste active à tout moment. Sinon, entrez le nombre de minutes que vous souhaitez laisser s'écouler avant interruption de votre connexion Internet. ▪ Keep Alive Cette option conserve votre connexion à Internet indéfiniment, même lorsque votre connexion est inactive. Cliquez sur le bouton radio situé en regard de Keep Alive. La période de recomposition par défaut est de 30 secondes (en d'autres termes, le routeur vérifiera la connexion Internet toutes les 30 secondes).

Champ	Description
	L2TP Le protocole de tunnellation couche 2 (L2TP) est un service qui concerne les connexions de tunnellation. ▪ DHCP À ne conserver que si votre ISP prend en charge DHCP ou si vous vous connectez via une adresse IP dynamique. ▪ Internet IP Address and Subnet Mask L'adresse IP et le masque de sous-réseau, tels qu'ils sont visibles par les utilisateurs externes sur Internet (notamment votre ISP). Si votre connexion Internet requiert une adresse IP statique, votre ISP vous fournira une adresse IP statique et un masque de sous-réseau. ▪ Gateway Votre ISP vous fournira l'adresse IP de la passerelle. ▪ DNS 1-3 Votre ISP vous fournira au moins une adresse IP du serveur DNS. Si vous souhaitez en utiliser une autre, entrez cette adresse IP dans l'un de ces champs. Vous pouvez entrer jusqu'à trois adresses IP du serveur DNS ici. Le routeur utilise ces dernières pour un accès plus rapide aux serveurs DNS en fonctionnement. ▪ Server IP Address Il s'agit de l'adresse IP du serveur L2TP. Entrez l'adresse IP qui vous a été communiquée par votre ISP. ▪ User Name and Password Entrez le nom d'utilisateur et le mot de passe fournis par votre ISP. ▪ Connect on Demand : inactivité maximale Si votre connexion Internet a été interrompue en raison de l'inactivité, Connect on Demand permet au routeur de rétablir automatiquement la connexion dès que vous essayez d'accéder à nouveau à Internet. ▪ Keep Alive Cette option conserve votre connexion à Internet indéfiniment, même lorsque votre connexion est inactive. La période de recomposition par défaut est de 30 secondes (en d'autres termes, le routeur vérifiera la connexion Internet toutes les 30 secondes).

Champ	Description
Host Name	Votre nom d'hôte. Il doit être au format : name.dyndns.org.
Domain Name	Votre nom de votre domaine. Il doit être au format : name.tzo.org.
MTU	La taille de l'unité de transfert maximale (MTU).
Static DNS 1 to 3	Les entrées 1 à 3 du système de noms de domaine (DNS). Le DNS correspond à la manière dont Internet traduit les noms de domaine ou de sites Web en adresses Internet ou URL. Votre ISP vous fournira au moins une adresse IP du serveur DNS. Si vous souhaitez en utiliser une autre, entrez cette adresse IP.

Page WAN Setup (ADSL)

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

- ÉTAPE 1** Cliquez sur **Quick Setup > WAN Setup**.
- ÉTAPE 2** La fenêtre *WAN Setup* s'ouvre.
- ÉTAPE 3** Entrez vos paramètres VC et IP selon les besoins.
- ÉTAPE 4** Cliquez sur **Submit** pour enregistrer les paramètres.

Champ	Description
Encapsulation	L'encapsulation est le protocole utilisé entre votre passerelle à haut débit et les serveurs de votre ISP. La plupart des encapsulations sont définies dans les normes Internet appelées « Requests For Comments » (RFC). Deux sont dérivées du protocole PPP (Point-to-Point) : PPP over Ethernet (PPPoE) et PPP over ATM (PPPoA).

Champ	Description
Multiplexing	Sélectionnez la méthode utilisée pour effectuer un routage des différents types de données via différents circuits virtuels (VC) vers le réseau ATM : encapsulation LLC (Logical Link Control, également appelée LLC-SNAP) ou multiplexage Virtual Channel (VC, également appelé VC-Mux).
QoS Type	Sélectionnez la méthode qualité de service (QoS) utilisée par votre ISP sur votre ligne : UBR (Unspecified Bit Rate)/ CBR (Constant Bit Rate), taux de transfert VBR en temps réel (RTVBR) ou taux de transfert VBR non en temps réel (NRTVBR). CBR offre la meilleure garantie de la faible latence ; UBR n'en offre aucune. ▪ Pcr Rate : quand QoS est défini sur CBR, VBR_RT ou VBR_NRT, le débit maximal des cellules (PCR) dans les cellules par seconde doit être entré ici. ▪ Scr Rate : quand QoS est défini sur VBR_NRT ou VBR_RT, le taux de cellules admissibles (SCR) dans les cellules par seconde doit être entré ici. ▪ MBS : quand QoS est défini sur VBR_NRT ou VBR_RT, les MBS dans les cellules par seconde doivent être entrées ici. ▪ CDVT : quand QoS est défini sur CBR, VBR_NRT ou VBR_RT, les CDVT dans les cellules par seconde doivent être entrées ici.
VPI/VCI Auto Detect	Vous pouvez activer ou désactiver la détection automatique des valeurs VPI et VCI (voir ci-dessous) qui identifient votre ligne au réseau ATM.
Virtual Circuit	Le VPI (Virtual Path Identifier) et le VCI (Virtual Channel Identifier) sont des valeurs utilisées pour identifier votre ligne au réseau ATM de votre ISP.
Static IP Setting	Sélectionnez cette option si votre ISP vous fournit une adresse IP statique. Entrez les informations requises suivantes, telles qu'elles vous sont fournies par votre ISP : Adresse IP Internet, masque de sous-réseau et adresse IP de la passerelle par défaut. En option, vous pouvez entrer les adresses IP de trois serveurs DNS au maximum ou laisser les champs vides pour permettre à un serveur DNS d'être choisi de manière dynamique.

Page LAN Setup

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

- ÉTAPE 1** Cliquez sur **Quick Setup > LAN Setup**. La fenêtre *LAN Setup* s'ouvre.
- ÉTAPE 2** Entrez votre type de connexion Internet et n'importe quel paramètre LAN facultatif, selon les besoins.
- ÉTAPE 3** Cliquez sur **Submit** pour enregistrer les paramètres.

Champ	Description
DHCP Name	Le nom DHCP.
Local IP Address / Subnet Mask	L'adresse IP et le masque de sous-réseau du DHCP, tels qu'ils sont visibles par les utilisateurs externes sur Internet (notamment votre ISP).
DHCP Server	Les paramètres du serveur DHCP. Cliquez sur le bouton Show DHCP Reservation pour modifier les paramètres du serveur DHCP.
Interface WAN	L'interface WAN.
Option 66	Option d'utilisation d'un serveur TFTP. Les options disponibles sont les suivantes : None, Local TFTP Server ou Remote TFTP Server. La valeur par défaut est None. ▪ L'option Local TFTP Server indique que la plate-forme prête pour les services est utilisée comme serveur TFTP pour ce sous-réseau LAN. ▪ L'option Remote TFTP Server indique que le serveur TFTP est obtenu sur l'interface WAN des plates-formes prêtes pour les services. ▪ L'option Manual TFTP Server indique qu'une adresse IP est entrée manuellement pour le serveur TFTP (autres que les plates-formes prêtes pour les services).
Option 67	Le nom du fichier de configuration à demander au serveur TFTP.

Champ	Description
Proxy DNS	Le proxy DNS relaie les requêtes DNS au serveur DNS du réseau public actuel pour le proxy et répond en tant que résolveur DNS au périphérique client sur le réseau. Pour activer la fonctionnalité du proxy DNS, sélectionnez Enabled . Le paramètre par défaut est Disabled .
Starting IP Address	Entrez une valeur avec laquelle commencer pour le serveur DHCP lors de la génération des adresses IP. Étant donné que l'adresse IP par défaut est 192.168.15.1, l'adresse IP de début doit être 192.168.15.2 ou supérieure, mais inférieure à 192.168.15.149. Par défaut, l'adresse IP de début est 192.168.15.100.
Maximum DHCP Users	Entrez le nombre maximal de PC auxquels vous souhaitez que le serveur DHCP attribue des adresses IP. Ce nombre ne peut pas être supérieur à 253. La valeur par défaut est 50.
IP Address Range	La plage d'adresses DHCP est affichée ici.
Client Lease Time	La durée pendant laquelle un utilisateur réseau sera autorisé à se connecter à la passerelle avec son adresse IP dynamique actuelle. Entrez la durée, en minutes, pendant laquelle l'utilisateur final « louera » cette adresse IP dynamique. Une fois cette durée écoulée, une nouvelle adresse IP dynamique sera automatiquement attribuée à l'utilisateur. La valeur par défaut est égale à 0 minutes, soit une journée.
Static DNS	Le système de noms de domaine (DNS) correspond à la manière dont Internet traduit les noms de domaine ou de sites Web en adresses Internet ou URL. Votre ISP vous fournira au moins une adresse IP du serveur DNS. Si vous souhaitez en utiliser une autre, entrez cette adresse IP.
WINS	Le serveur WINS (Windows Internet Naming Service) gère l'interaction des PC avec Internet. Si vous utilisez un serveur WINS, entrez l'adresse IP du serveur ici. Autrement, ne renseignez pas ce champ.

Page Wireless Setup

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

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

ÉTAPE 2 Dans le champ Network Mode, sélectionnez un mode réseau sans fil.

- Si vous avez des périphériques sans fil-N, sans fil-G et sans fil-B dans votre réseau, utilisez le paramètre par défaut, **Mixed**.
- Si vous avez uniquement des périphériques sans fil-G et sans fil-B dans votre réseau, sélectionnez BG-Mixed. Si vous avez uniquement des périphériques sans fil-N, sélectionnez **Wireless-N Only**.
- Si vous avez uniquement des périphériques sans fil-G, sélectionnez **Wireless-G Only**.
- Si vous avez uniquement des périphériques sans fil-B, sélectionnez **Wireless-B Only**.
- Si vous n'avez pas de périphérique sans fil dans votre réseau, sélectionnez **Disabled**.

ÉTAPE 3 Dans le champ Radio Band, sélectionnez une bande passante pour le réseau sans fil.

ÉTAPE 4 Si nécessaire, sélectionnez un canal qui appartient au type de bande passante que vous avez sélectionné dans l'étape précédente.

ÉTAPE 5 Si nécessaire, ajoutez ou modifiez le nom du réseau sans fil (SSID).

ÉTAPE 6 Cliquez sur **Edit** pour activer la sécurité pour le SSID. Cisco vous recommande vivement d'activer la sécurité pour chaque SSID.

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

Champ	Description
Network Mode	Le mode réseau. Le mode par défaut est Mixed .
Radio Band	La bande passante du canal radio. La valeur par défaut est Standard - 20MHz Channel .

Champ	Description
Wide Channel	Si vous avez sélectionné Wide - 40MHz Channel pour le paramètre Radio Band, ce dernier est disponible pour votre canal sans fil-N principal. Sélectionnez n'importe quel canal dans le menu déroulant.
Standard Channel	Si vous avez sélectionné Wide - 40MHz Channel ou Standard -20MHz Channel pour le paramètre Radio Band, ce dernier 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 Channel pour le paramètre Radio Band, le canal standard est un canal auxiliaire pour le réseau sans fil-N. La valeur par défaut est channel 11.
Wireless Network Name (SSID)	Le premier réseau sans fil par défaut utilise le nom « cisco_data », connecté au VLAN par défaut. Le deuxième réseau sans fil par défaut utilise le nom « cisco_voice », connecté au VLAN voip. Pour renommer le réseau sans fil par défaut, entrez un nom du réseau sans fil unique, sensible à la casse et ne devant pas dépasser 32 caractères (utilisez n'importe quels caractères du clavier).
Broadcast Network Name	Lorsque les clients sans fil recherchent les réseaux sans fil locaux pour s'y associer, ils détectent la diffusion SSID par la passerelle. Si vous souhaitez diffuser SSID, maintenez la case cochée. Si vous ne souhaitez pas diffuser le SSID, décochez la case.
Enabled Network	Pour activer le réseau sans fil, cochez la case. Pour désactiver le réseau sans fil, décochez la case.
WPS Hardware Button	Pour activer le bouton WPS Hardware situé en haut du SRP, cochez la case.
Edit	Cliquez sur le bouton Edit pour définir le mode de sécurité pour le SSID. Chaque mode est décrit ci-dessous.

Champ	Description
Edit (suite)	▪ WEP : méthode de cryptage de base offrant deux niveaux de cryptage : un cryptage à 128 bits est plus fort qu'un cryptage à 64 bits. - Authentication Type : le type par défaut est Auto, qui permet l'authentification en système ouvert ou clé partagée. Avec l'authentification en système ouvert, l'expéditeur et le destinataire N'utilisent PAS de clé WEP pour l'authentification. Avec l'authentification en clé partagée, l'expéditeur et le destinataire utilisent une clé WEP pour authentification. Sélectionner Shared Key only permet l'authentification en clé partagée. - Encryption : sélectionnez le niveau adéquat du cryptage, 64 bits (10 chiffres hexadécimaux) ou 128 bits (26 chiffres hexadécimaux). - Passphrase : pour générer des clés automatiquement, entrez un mot de passe et cliquez sur le bouton Generate. - Key 1-4 : si vous souhaitez entrer manuellement les clés WEP, entrez-les ensuite dans les champs Key 1-4. - TX Key : pour indiquer la clé WEP à utiliser, sélectionnez un numéro de clé de transmission.

Champ	Description
Edit (suite)	▪ WPA Personal : accès protégé par Wi-Fi (WPA - Wi-Fi Protected Access) est une toute nouvelle norme de sécurité relative à la sécurisation des communications sans fil. - WPA Algorithms : sélectionnez l'algorithme que vous souhaitez utiliser, TKIP ou AES. (AES est une méthode de cryptage plus forte que la technologie TKIP.) - WPA Shared Key : entrez la clé partagée par le routeur et vos autres périphériques réseau. Elle doit compter entre 8 et 63 caractères ASCII ou 64 caractères hexagonaux. - Group Key Renewal : entrez la période de renouvellement des clés, pour indiquer au routeur la fréquence à laquelle il doit modifier les clés de cryptage.
Edit (suite)	▪ WPA2 Personal - WPA Algorithms : sélectionnez le ou les algorithmes que vous souhaitez utiliser, AES ou TKIP + AES. (AES est une méthode de cryptage plus forte que la technologie TKIP.) - WPA Shared Key : entrez la clé partagée par le routeur et vos autres périphériques réseau. Elle doit compter entre 8 et 63 caractères ASCII ou 64 caractères hexagonaux. - Group Key Renewal : entrez la période de renouvellement des clés, pour indiquer au routeur la fréquence à laquelle il doit modifier les clés de cryptage.

Champ	Description
Edit (suite)	▪ WPA Entreprise : cette option propose le WPA utilisé en coordination avec un serveur RADIUS. Si vous avez deux serveurs RADIUS, sélectionnez-en un comme serveur principal, puis indiquez un serveur secondaire à utiliser en tant que serveur de sauvegarde. (Cette option doit uniquement être utilisée lorsqu'un serveur RADIUS est accessible depuis le routeur.) - WPA Algorithms : sélectionnez le ou les algorithmes que vous souhaitez utiliser, TKIP ou AES. (AES est une méthode de cryptage plus forte que la technologie TKIP.) - RADIUS Server Address (Primary and Secondary) : entrez l'adresse IP de votre serveur RADIUS. - RADIUS Port : entrez le numéro de port de votre serveur RADIUS. - Shared Secret : entrez la clé partagée par le routeur et le serveur RADIUS. La clé peut compter entre 8 et 63 caractères ASCII ou 64 caractères hexagonaux. - Key Renewal Timeout : entrez la période de renouvellement des clés, pour indiquer au routeur la fréquence à laquelle il doit modifier les clés de cryptage.

Champ	Description
Edit (suite)	▪ WPA2 Entreprise : cette option propose le WPA2 utilisé en coordination avec un serveur RADIUS. (Ceci doit uniquement être utilisé lorsqu'un serveur RADIUS est connecté au routeur.) - WPA Algorithms : sélectionnez le ou les algorithmes que vous souhaitez utiliser, AES ou TKIP + AES. (AES est une méthode de cryptage plus forte que la technologie TKIP.) - RADIUS Server Address (Primary and Secondary) : entrez l'adresse IP de votre serveur RADIUS. - RADIUS Port : entrez le numéro de port de votre serveur RADIUS. - Shared Secret : entrez la clé partagée par le routeur et le serveur RADIUS. La clé peut compter entre 8 et 63 caractères ASCII ou 64 caractères hexagonaux. - Key Renewal Timeout : entrez la période de renouvellement des clés, pour indiquer au routeur la fréquence à laquelle il doit modifier les clés de cryptage.
Edit (suite)	Disabled : aucune sécurité n'est définie pour le SSID. Cette option n'est pas recommandée par Cisco.

Page Remote Provisioning

Cette fonctionnalité vous permet de configurer la communication avec un serveur de contrôle d'accès (ACS) via le protocole de gestion des réseaux WAN (CWMP) CPE TR-069.

- ÉTAPE 1** Cliquez sur **Quick Setup > Remote Provisioning**. La fenêtre *Remote Provisioning* s'ouvre.
- ÉTAPE 2** Cliquez sur **Enabled** pour activer la mise en service à distance.
- ÉTAPE 3** Entrez l'URL pour l'ACS. Le format doit être `http(s)://xxx.xxx.xxx.xxx:port` or `xxx.xxx.xxx.xxx:port`. `xxx.xxx.xxx.xxx` est le nom de domaine ou l'adresse IP du serveur ACS et le port se trouve après « : ». L'adresse IP et le port doivent être renseignés.

ÉTAPE 4 Entrez le nom d'utilisateur et le mot de passe ACS.

ÉTAPE 5 En option, entrez le nom d'utilisateur et le mot de passe utilisés pour la demande de connexion.

ÉTAPE 6 En option, entrez l'intervalle d'information périodique.

ÉTAPE 7 Cliquez sur Submit pour enregistrer les paramètres.

Champ	Description
Status	Sélectionnez une option pour activer ou désactiver la mise en service à distance.
ACS URL	L'URL de l'ACS. Le format doit être http(s)://xxx.xxx.xxx.xxx:port or xxx.xxx.xxx.xxx:port. xxx.xxx.xxx.xxx est le nom de domaine ou l'adresse IP du serveur ACS et le port se trouve après « : ». L'adresse IP et le port doivent être renseignés.
ACS Username	Le nom d'utilisateur pour l'ACS. Le nom d'utilisateur par défaut est OUI Serial Number ; il doit être identique à celui configuré côté ACS et doit être renseigné.
ACS Password	Le mot de passe pour l'ACS. Il doit être identique à celui configuré côté ACS et doit être renseigné.
Connection Request URL	Ce champ est renseigné automatiquement et n'a donc pas besoin d'être renseigné manuellement. Le format est http://xxx.xxx.xxx.xxx:port. xxx.xxx.xxx.xxx est l'adresse IP du WAN du CPE.
Connection Request Username	Nom d'utilisateur de la demande de connexion. Il doit être identique à celui configuré côté ACS.
Connection Request Password	Mot de passe de la demande de connexion. Il doit être identique à celui configuré côté ACS.
Periodic Inform Interval	L'intervalle d'information périodique. La valeur par défaut est de 86400 secondes.
Periodic Inform Enable	Pour activer ou désactiver l'information périodique.
Request Download	Si appliqué, l'ACS peut appeler le RPC de téléchargement une fois qu'il reçoit la demande du CPE.

Configuration avancée

Les fonctionnalités Advanced Configuration Setup vous permettent de configurer les paramètres avancés avec la voix, la configuration du réseau mobile, le pare-feu et le NAT.

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

Option Voice

L'option Voice vous permet d'administrer et d'afficher les paramètres de voix. Pour plus d'informations, reportez-vous à la section **Configuration de la voix, page 103**

Option Mobile Network Setup

L'option Mobile Network Setup vous permet d'administrer les paramètres réseau mobile. Pour plus d'informations, reportez-vous à la section **Page Mobile Network, page 44**.

Option Firewall

L'option Firewall vous permet d'administrer les paramètres du filtre de pare-feu. Pour plus d'informations, reportez-vous à la section **Page Firewall, page 89**.

Option NAT

L'option NAT vous permet d'administrer les paramètres NAT. Pour plus d'informations, reportez-vous à la section **Page NAT, page 80**.

Configuration des interfaces des plates-formes prêtes pour les services

Ce chapitre décrit comment configurer les interfaces pour votre SRP. Il comprend les sections suivantes :

- **Configuration de l'interface WAN**
- **Configuration des interfaces VLAN et des ports WAN**
- **Configuration du 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 de l'interface WAN

Cette section décrit comment configurer les paramètres d'interface WAN pour la SRP, notamment :

- **Page Internet Setup**
- **Page Mobile Network**
- **Page Failover & Recovery (SRP521W)**
- **Page Failover & Recovery (SRP526W, SRP527W)**

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 cela, reportez-vous à la section **Page User List, page 225**. 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.
- ÉTAPE 2 Pour ajouter ou modifier des interfaces dans la liste des interfaces WAN, cliquez sur les icônes d'ajout ou de modification.
- ÉTAPE 3 Modifiez les paramètres de port selon les besoins.
- ÉTAPE 4 Pour cloner une adresse MAC pour la SRP, cliquez sur **Enabled**, puis entrez une adresse MAC. Pour cloner l'adresse MAC de votre ordinateur, cliquez sur le bouton **Clone Your PC's MAC**.
- ÉTAPE 5 Cliquez sur **Submit** pour enregistrer les paramètres.

Champ	Description
WAN Interface List	Liste des interfaces WAN indiquant le lien physique, son protocole et son adresse IP (le cas échéant). Dans chaque entrée, vous pouvez créer une nouvelle sous-interface en cliquant sur le bouton Add Subinterface ou sur le bouton Edit. Si vous disposez de plusieurs sous-interfaces, vous pouvez choisir l'une d'entre elles comme interface de routage par défaut en cochant la case d'option Default Route.
Flow Control	Permet de contrôler le flux du WAN. Pour définir le contrôle du flux du WAN, sélectionnez Enabled et cliquez sur Submit. Le paramètre par défaut est Disabled.

Champ	Description
Speed Duplex	Permet d'activer le mode de débit-duplex pour le WAN. Les choix possibles sont Auto-negotiate, 10 Half, 10 Full, 100 Half et 100 Full. Pour définir le mode de débit-duplex pour le WAN, choisissez ce mode et cliquez sur Submit. Le paramètre par défaut est Auto-negotiate.
MAC Address Clone	Une adresse MAC est composée d'un code à 12 chiffres attribué à un composant matériel unique en vue de son identification. Certains ISP exigent que vous enregistriez une adresse MAC pour accéder à Internet. Si vous ne souhaitez pas ré-enregistrer d'adresse MAC auprès de votre ISP, vous pouvez attribuer à la SRP l'adresse MAC actuellement enregistrée auprès de votre ISP avec la fonctionnalité de clonage de l'adresse MAC. Pour cloner votre adresse MAC, sélectionnez Enabled, cliquez sur Clone Your PC's MAC, puis sur Submit. La valeur par défaut est Disabled.
WAN Interface Detail	La zone Details of WAN contient des informations à propos de votre WAN.

Lorsque vous choisissez une nouvelle interface ou que vous en modifiez une existante à l'aide des icônes d'ajout ou de modification, l'une des options de VC suivantes peut être disponible.

Paramètres VC

Champ	Description
Multiplexing	Le multiplexage définit la manière dont les différents protocoles sont gérés dans un circuit DSL virtuel. Vous avez le choix entre l'encapsulation LLC (Logical Link Control, également appelée LLC-SNAP) ou le multiplexage VC (Virtual Channel, également appelé VC-Mux).
QoS Type	Sélectionnez la méthode qualité de service (QoS) DSL utilisée par votre ISP sur votre ligne : UBR (Unspecified Bit Rate), CBR (Constant Bit Rate), taux de transfert VBR en temps réel (RTVBR) ou taux de transfert VBR non en temps réel (NRTVBR). CBR offre la meilleure garantie en termes 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 : quand 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 : quand la QoS est définie sur VBR_NRT ou VBR_RT, entrez ici le taux de cellules admissibles (SCR) dans les cellules par seconde. ▪ MBS : quand la QoS est définie sur VBR_NRT ou VBR_RT, entrez ici les MBS dans les cellules par seconde. ▪ CDVT : quand la QoS est définie sur CBR, VBR_NRT ou VBR_RT, entrez ici les CDVT dans les cellules par seconde.
VPI/VCI Auto Detect	Vous pouvez activer ou désactiver la détection automatique des valeurs VPI et VCI qui identifient votre ligne auprès du réseau ATM. Le VPI (Virtual Path Identifier) et le VCI (Virtual Channel Identifier) sont des valeurs utilisées pour identifier votre ligne auprès du réseau ATM de votre ISP. La SRP détecte automatiquement les services DSL offerts sur les paires VC suivantes : 0/35, 8/35, 0/43, 0/51, 0/59, 8/43, 8/51, 8/59, 0/38

Paramètres IPOA / Static IP

Sélectionnez l'option IPOA Settings / Static IP Setting si votre ISP vous a fourni une adresse IP statique. 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. En option, vous pouvez entrer les adresses IP de trois serveurs DNS au maximum ou laisser les champs vides pour permettre à un serveur DNS d'être sélectionné de manière dynamique.

Champ	Description
Internet IP Address and Subnet Mask	Adresse IP et masque de sous-réseau de la SRP, tels qu'ils apparaissent pour les utilisateurs externes sur 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	Sert à définir un ou deux serveurs DNS. La SRP les utilise 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 ATM DSL virtuel. Saisissez le nom d'utilisateur et le mot de passe fournis par votre ISP. En option, vous pouvez également spécifier le nom du service PPP, s'il vous a été fourni par votre prestataire de services.

Champ	Description
Service Name	(PPPoE uniquement.) Un nom de service est une chaîne requise par certains ISP. Renseignez ce champ uniquement si cela est requis par votre ISP.
User name and Password	Saisissez les chaînes que votre ISP vous a demandé d'utiliser. Le nom d'utilisateur peut s'appeler « nom utilisateur », « identifiant de connexion » ou « nom de connexion ».
Connect on Demand	Cliquez sur cette option si vous souhaitez 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 de 20 minutes. Au lieu de choisir l'option Connect on Demand, vous pouvez choisir l'option Keep Alive (voir ci-dessous). Dans la plupart des cas, vous pouvez choisir l'une ou l'autre option sans avoir à consulter votre ISP.

Champ	Description
Keep Alive	Cliquez sur cette option si vous souhaitez 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.
Enable MTU/MRU greater than 1492	Informations d'en-tête supplémentaires utilisées sur les connexions PPPoE par ADSL qui limitent à 1492 octets la taille maximale de paquet pouvant être envoyée. Activez ce paramètre uniquement si votre ISP vous le demande.

Paramètres PPPoA

Champ	Description
User name et Password	Saisissez les chaînes que votre ISP vous a demandé d'utiliser. Le nom d'utilisateur peut s'appeler « nom utilisateur », « identifiant de connexion » ou « nom de connexion ».
Connect on Demand	Cliquez sur cette option si vous souhaitez 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 de 20 minutes. Au lieu de choisir l'option Connect on Demand, vous pouvez choisir l'option Keep Alive (voir ci-dessous). Dans la plupart des cas, vous pouvez choisir l'une ou l'autre option sans avoir à consulter votre ISP.
Keep Alive	Cliquez sur cette option si vous souhaitez 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.

Page Mobile Network

La page Mobile Network permet de configurer les paramètres de réseau mobile. Vous pouvez configurer votre SRP afin qu'elle se connecte à un modem large bande mobile USB, connecté à son interface USB. Pour obtenir des informations sur les modems compatibles, consultez l'adresse suivante : www.cisco.com/go/srp500.

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

ÉTAPE 2 Vous pouvez, si nécessaire, modifier les paramètres globaux dans la zone Global Settings. Le champ **Card Status** indique l'état de votre carte mobile.

ÉTAPE 3 Vous pouvez, si nécessaire, modifier les paramètres de réseau mobile dans la zone **Mobile Network Setup**.

REMARQUE Cliquez sur l'option **Manual** dans le champ Configure Mode pour configurer manuellement votre carte de réseau mobile.

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

Champ	Description
Connect Mode	Choisissez le mode Auto ou Manual. 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. REMARQUE Sur la SRP521W, les fonctionnalités de récupération de connexion Ethernet et de basculement de connexion d'interface fonctionnent uniquement si le mode de connexion est défini sur Auto. Si vous sélectionnez l'option Auto, vous devez sélectionner Connect on Demand et Keep Alive. Si vous sélectionnez l'option Connect on Demand, vous pouvez configurer la SRP afin de mettre fin à la connexion Internet lorsqu'elle est inactive pendant une période définie (inactivité maximale).

Champ	Description
Connect on Demand	Sélectionnez cette option pour que la SRP mette fin à la connexion Internet lorsqu'elle est inactive pendant une période définie (inactivité maximale). Si votre connexion Internet a été interrompue en raison d'une inactivité, l'option Connect on Demand permet au modem de rétablir automatiquement cette connexion dès qu'un utilisateur essaie d'accéder à nouveau à Internet. Dans le champ Max Idle Time, saisissez le nombre de minutes devant s'écouler avant qu'une connexion Internet soit interrompue. Le délai d'inactivité maximal par défaut est de 5 minutes.
Tunnel Protocol	Le protocole de tunnel (PPTP/L2TP) est pris en charge via un modem USB par l'une de ces méthodes. ▪ NONE. Sélectionnez cette option pour désactiver le protocole de tunnellation. ▪ PPTP/L2TP. Sélectionnez PPTP ou L2TP selon le service que vous souhaitez utiliser. Vous devez fournir l'adresse IP du serveur, le nom d'utilisateur et le mot de passe. ▪ Follow Ethernet WAN configure. Sélectionnez cette option pour que le protocole de tunnel suive la configuration du WAN Ethernet.

Champ	Description
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). Ces messages peuvent également s'afficher : - Please set APN manually Ce message s'affiche lorsque la SRP ne parvient pas à déterminer l'APN à partir 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 - error REMARQUE Si le champ Connect Mode est défini sur Manual, vous pouvez cliquer sur un bouton pour connecter ou déconnecter votre modem.
Configure Mode	La SRP détecte automatiquement les modems pris en charge et présente la liste des configurations appropriées par défaut. Pour remplacer l'un de ces paramètres (à l'exception du code PIN de la carte SIM), sélectionnez le mode de configuration manuel.
Card Model	Modèle de carte de données inséré dans le lecteur USB.

Champ	Description
Carrier	Prestataire de services de réseau mobile pour la connexion Internet. Ce paramètre est requis lorsque vous utilisez un service Internet HSDPA/UMTS/GPRS. Sélectionnez le pays d'émission de la carte dans la première liste déroulante, puis sélectionnez le fournisseur qui l'a émise dans la deuxième liste déroulante.
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.
Dial Number	Numéro à composer pour la connexion internet. Entrez le numéro fourni par votre prestataire de services de réseau mobile.
User Name/ Password	Saisissez le nom d'utilisateur et le mot de passe fournis par votre prestataire de services de réseau mobile.
SIM PIN	Code PIN associé à votre carte SIM. Saisissez le code PIN de votre carte SIM dans ce champ. Ce champ s'affiche uniquement pour les cartes GSM.
Server Name	Nom du serveur pour 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 méthode par défaut est Auto. Si vous ne savez pas quel type d'authentification utiliser, conservez le paramètre par défaut.
Service Type	Sélectionnez le type de connexion de services de données mobiles disponible le plus courant, en fonction du signal de service de votre zone. Si un seul service de données mobiles est pris en charge là où vous vous trouvez, vous pouvez configurer une connexion améliorée. La première sélection recherche toujours le service HSDPA/3G/UMTS ou bascule automatiquement sur le service GPRS uniquement lorsqu'il est disponible.

Page Failover & Recovery (SRP521W)

Une connexion Internet peut être établie via le port WAN ou un modem sans fil branché au port USB. Consultez le site www.cisco.com/go/srp500 pour plus d'informations sur les modems compatibles USB.

Il est possible de connecter à la fois un modem Ethernet et un modem USB, mais un seul d'entre eux peut être utilisé pour établir un lien. Lorsque la connexion Internet échoue, la SRP essaie automatiquement d'établir une autre connexion sur une autre interface. Cette fonctionnalité s'appelle le *basculement*. Dès que la connexion Internet par Ethernet est restaurée, la SRP essaie automatiquement de rétablir la connexion Internet. Cette fonctionnalité s'appelle la *récupération*.

ÉTAPE 1 Cliquez sur **Interface Setup > Failover & Recovery**. La fenêtre *Failover & Recovery* s'ouvre.

ÉTAPE 2 Si nécessaire, activez la fonctionnalité de récupération de connexion Ethernet en cliquant sur **Enabled**.

Lorsque cette option est activée, la SRP définit l'interface Ethernet sur la priorité la plus élevée. Lorsque vous activez cette fonctionnalité, celle de basculement de la connexion d'interface est également activée. Lorsque la connexion Internet échoue, la SRP essaie automatiquement de rétablir la connexion de réseau mobile sur l'interface USB (si disponible). Dès que la connexion Internet par Ethernet est restaurée, la SRP essaie automatiquement de rétablir la connexion Internet par Ethernet.

REMARQUE Le mode de connexion mobile doit être défini sur Auto pour utiliser la fonctionnalité de récupération de connexion Ethernet.

ÉTAPE 3 Si nécessaire, saisissez une valeur de temporisation Ethernet.

ÉTAPE 4 Dans la zone Failover Validation Site, choisissez un site sur lequel effectuer une validation du basculement. Utilisez la SRP ou entrez l'adresse IP d'un site personnalisé.

ÉTAPE 5 Si nécessaire, modifiez la priorité des interfaces WAN en cliquant sur les boutons du **haut** ou du **bas**.

ÉTAPE 6 Cliquez sur Submit pour enregistrer les paramètres.

Paramètres de basculement et de récupération (SRP521W)

Champ	Description
Ethernet Connection Recovery	Cette fonctionnalité garantit que votre connexion Internet par Ethernet est toujours connectée lorsqu'elle est disponible.
Interface Connection Failover	La détection du basculement fonctionne par la détection de la connexion physique et/ou de la présence de trafic sur le lien Internet. Si le lien est inactif, la SRP tente d'effectuer un test ping sur une destination. Si le test ping ne répond pas, la SRP suppose que le lien est défaillant et tente de basculer sur une autre interface.
Timeout	Intervalle auquel la SRP détecte l'état de la connexion Internet. L'intervalle par défaut est de 60 secondes.
Connection Validation Site	Cible du ping que la SRP doit utiliser pour détecter l'état de la connexion internet. Par défaut la SRP exécute une commande ping sur les serveurs NTP (Network Time Protocol). Vous pouvez spécifier une adresse IP différente comme cible dans ce champ.
WAN Interfaces	Ce champ fournit des informations sur l'état actuel de la connexion Internet par Ethernet et de la connexion réseau mobile. Vous pouvez cliquer sur le lien hypertexte de l'état pour afficher les détails. Vous pouvez également configurer la priorité d'interface en cliquant sur Up ou Down. Notez que le paramètre de priorité d'interface est configurable uniquement lorsque la fonctionnalité de récupération de connexion Ethernet est désactivée.

Page Failover & Recovery (SRP526W, SRP527W)

Une connexion Internet peut être établie via le port DSL ou un modem sans fil branché au port USB. Consultez le site www.cisco.com/go/srp500 pour plus d'informations sur les modems compatibles USB.

Il est possible de connecter à la fois un modem DSL et un modem USB 3G, mais un seul d'entre eux peut être utilisé pour établir un lien. Lorsque la connexion Internet échoue, la SRP essaie automatiquement d'établir une autre connexion sur une autre interface. Cette fonctionnalité s'appelle le *basculement*. Dès que la connexion Internet DSL est restaurée, la SRP essaie automatiquement de rétablir la connexion Internet. Cette fonctionnalité s'appelle la *récupération*.

ÉTAPE 1 Cliquez sur **Interface Setup > Failover & Recovery**. La fenêtre *Failover & Recovery* s'ouvre.

ÉTAPE 2 Si nécessaire, activez la fonctionnalité de récupération de connexion Ethernet en cliquant sur **Enabled**.

Lorsque cette option est activée, la SRP définit l'interface Ethernet sur la priorité la plus élevée. Lorsque vous activez cette fonctionnalité, celle de basculement de la connexion d'interface est également activée. Lorsque la connexion Internet échoue, la SRP essaie automatiquement de rétablir la connexion de réseau mobile sur l'interface USB (si disponible). Dès que la connexion Internet par Ethernet est restaurée, la SRP essaie automatiquement de rétablir la connexion Internet par Ethernet.

REMARQUE Le mode de connexion mobile doit être défini sur Auto pour utiliser la fonctionnalité de récupération de connexion Ethernet.

ÉTAPE 3 Si nécessaire, saisissez une valeur de temporisation Ethernet.

ÉTAPE 4 Dans la zone Failover Validation Site, choisissez un site sur lequel effectuer une validation du basculement. Utilisez la SRP ou entrez l'adresse IP d'un site personnalisé.

ÉTAPE 5 Si nécessaire, modifiez la priorité des interfaces WAN en cliquant sur les boutons du **haut** ou du **bas**.

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

Paramètres de basculement et de récupération (SRP526W/SRP527W)

Champ	Description
Connection Recovery	Cette fonctionnalité garantit que votre connexion Internet est toujours connectée lorsqu'elle est disponible.
Interface Connection Failover	La détection du basculement fonctionne par la détection de la connexion physique et/ou de la présence de trafic sur le lien Internet. Si le lien est inactif, la SRP tente d'effectuer un test ping sur une destination. Si le test ping ne répond pas, la SRP suppose que le lien est défaillant et tente de basculer sur une autre interface.
Timeout	Intervalle auquel la SRP détecte l'état de la connexion Internet. L'intervalle par défaut est de 60 secondes.
Connection Validation Site	Cible du ping que la SRP doit utiliser pour détecter l'état de la connexion internet. Par défaut la SRP exécute une commande ping sur les serveurs NTP (Network Time Protocol). Vous pouvez spécifier une adresse IP différente comme cible dans ce champ.
WAN Interfaces	Ce champ fournit des informations sur l'état actuel de la connexion Internet et de la connexion réseau mobile. Vous pouvez cliquer sur le lien hypertexte de l'état pour afficher les détails. Vous pouvez également configurer la priorité d'interface en cliquant sur Up ou Down. Notez que le paramètre de priorité d'interface est configurable uniquement lorsque la fonctionnalité de récupération de connexion est désactivée.

Configuration des interfaces VLAN et des ports WAN

Cette section décrit comment installer les ports VLAN et LAN de la SRP. Il comprend les sections suivantes :

- **Page DHCP Server**
- **Page VLAN Setting**
- **Page Port Settings**

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

Page DHCP Server

Pour configurer la SRP en tant que serveur DHCP, vous devez tout d'abord créer un serveur DHCP via la page DHCP Server, puis l'activer en l'affectant à une interface VLAN.

REMARQUE Lorsque vous créez un serveur DHCP, vous devez également spécifier l'adresse IP et le masque de l'interface VLAN à laquelle il est affecté. Si vous n'affectez pas de serveur DHCP à une interface VLAN, les options d'adressage IP sont alors configurées directement via les paramètres VLAN.

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

-
- ÉTAPE 1** Cliquez sur **Interface Setup > LAN > DHCP Server**. La fenêtre *DHCP Server* s'ouvre.
- ÉTAPE 2** Pour afficher les informations d'une entrée DHCP, cliquez sur l'un des éléments de la liste de DHCP. Les informations DHCP s'affichent dans le tableau **DHCP Details**.
- ÉTAPE 3** Pour ajouter ou supprimer une entrée DHCP de la liste de DHCP, cliquez sur l'icône **Edit** (stylo) ou **Delete** (x) .
- ÉTAPE 4** Pour créer un nouveau pool de serveurs DHCP, cliquez sur **Add Entry**. La fenêtre *DCHP Server* de la nouvelle entrée s'ouvre.
- ÉTAPE 5** Under Router IP, enter the **DHCP Name** and **Local IP Address/Subnet Mask**.
- ÉTAPE 6** Configurez les paramètres du serveur DHCP tels que définis dans le tableau **Paramètres du serveur DHCP**.
- ÉTAPE 7** Cliquez sur **Submit** pour enregistrer les paramètres.
-

Paramètres du serveur DHCP	
Champ	Description
Router IP	
DHCP Name	Étiquette qui identifie la configuration du serveur DHCP et qui est utilisée pour affecter le service à une interface VLAN.
Local IP Address/ Subnet Mask	Adresse IP et masque de sous-réseau utilisés pour configurer l'interface VLAN à laquelle cette règle DHCP s'applique.
DHCP Server Setting	
Show DHCP Reservation button	Cliquez sur ce bouton pour vérifier et modifier les réservations DHCP. Cliquez à nouveau sur ce bouton pour masquer les tableaux de réservation.
WAN Interface	Choisissez l'interface WAN à partir de laquelle les informations de DHCP (en particulier DNS) sont obtenues.
Option 66	Fournit les informations d'adresse du serveur de mise en service aux hôtes qui en font la demande. Les informations relatives au serveur peuvent être définies de l'une de ces trois manières : ▪ Serveur TFTP local : La SRP utilise son propre serveur TFTP pour trouver les fichiers de mise en service, il renvoie donc sa propre adresse IP locale au client. ▪ Serveur TFTP distant : Si la SRP a été configurée à l'aide de cette méthode, elle utilise les informations relatives au serveur qu'elle a reçues via l'option 66 sur son interface WAN en réponse aux demandes du client local. ▪ Serveur TFTP manuel : 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 accepte et offre également une URL complète (comprenant le protocole, le chemin et le nom de fichier) pour répondre aux besoins de clients spécifiques.

Paramètres du serveur DHCP	
Champ	Description
Option 67	Fournit une configuration/un nom du fichier d'amorçage aux hôtes qui en font la demande. Cette option est utilisée conjointement avec l'option 66 pour autoriser le client à former une demande TFTP appropriée pour le fichier.
Proxy DNS	Si le proxy DNS est activé, les clients locaux peuvent utiliser l'adresse IP locale de la SRP 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 à propos du DNS dans la section Page Internet Setup, page 39. Si le proxy DNS est désactivé, les clients DHCP se voient proposer les informations du serveur DNS en fonction des éléments suivants : ▪ Si le champ Static DNS est configuré, alors seul le serveur est proposé aux clients. ▪ Si le champ Static DNS n'est pas configuré, jusqu'à trois serveurs sont proposés, tout d'abord à partir de la configuration statique des options Internet globales, puis à partir de l'interface WAN désignée ci-dessus.
Starting IP Address	Saisissez l'adresse IP de la première adresse dans ce pool.
Maximum DHCP Users	Entrez le nombre maximal de périphériques auxquels vous souhaitez que le serveur DHCP attribue des adresses IP. Le masque de sous-réseau et l'adresse IP de début affectent ce nombre. Ce nombre ne peut pas être supérieur à 1024. La valeur par défaut est 50.
IP Address Range	La plage d'adresses DHCP est affichée ici.
Client Lease Time	Durée pendant laquelle une adresse est louée à un client. Saisissez la durée du bail, en minutes. La valeur par défaut est égale à 0 minute, soit une journée. Saisissez 9999 pour attribuer un bail à durée indéfinie.

Paramètres du serveur DHCP	
Champ	Description
Static DNS	Permet de définir une adresse de serveur DNS que les clients DHCP doivent utiliser directement pour la résolution de noms. Cette option est uniquement requise lorsque la fonctionnalité du proxy DNS est désactivée pour ce serveur DHCP. Ce champ est masqué lorsque le proxy DNS est activé.
WINS	Le serveur WINS (Windows Internet Naming Service) gère le nom d'hôte de la fenêtre pour la résolution d'adresse. Si vous utilisez un serveur WINS, entrez l'adresse IP du serveur ici. Autrement, ne renseignez pas ce champ.

Page VLAN Setting

Les paramètres VLAN sont configurés sur cette page. Après avoir cliqué sur Add Entry, vous pouvez créer un autre VLAN.

- ÉTAPE 1** Cliquez sur **Interface Setup > LAN > VLAN Setting**. La fenêtre *VLAN Setting* s'ouvre. Vous pouvez modifier ou supprimer une entrée de VLAN en cliquant sur l'icône de modification ou de suppression.

Sur cette page, vous pouvez afficher la liste des VLAN configuré, ajouter ou supprimer un VLAN et afficher les informations détaillées d'un VLAN sélectionné.
- ÉTAPE 2** Pour modifier ou supprimer une entrée de VLAN de la liste de DHCP, cliquez sur l'icône **Edit** (stylo) ou **Delete (x)**.
- ÉTAPE 3** Pour afficher les informations d'une entrée de VLAN, cliquez sur un élément quelconque dans la liste **VLAN Details**. Les informations relatives au VLAN du pool de DHCP s'affichent dans le tableau **VLAN Details**.
- ÉTAPE 4** Pour créer nouveau VLAN, cliquez sur **Add Entry**. La fenêtre *VLAN Settings* du nouveau VLAN s'ouvre.
- ÉTAPE 5** Indiquez les paramètres VLAN de la nouvelle entrée tels que définis dans le tableau **Paramètres VLAN**.
- ÉTAPE 6** Cliquez sur **Submit** pour enregistrer les paramètres.
- ÉTAPE 7** Cliquez sur **Add Entry** pour ouvrir la page VLAN Add. À partir de cette page, vous pouvez ajouter une entrée de VLAN.
- ÉTAPE 8** Cliquez sur **Submit** pour enregistrer les paramètres.

Paramètres VLAN	
Champ	Description
VLAN Name	Nom du pont ou du VLAN.
VLAN ID	ID du pont ou du VLAN.
Voice VLAN	Cochez cette case si vous souhaitez utiliser la voix. Utilisez cette option uniquement en mode VLAN.
Address Type	Le type d'adresse 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 lors du pontage de ports uniquement. - Choisissez Static IP Address pour définir manuellement une adresse pour l'interface ou bien Dynamic IP Address pour demander une adresse à partir d'un serveur DHCP sur le réseau local. Sélectionnez DHCP server pour activer un service de serveur DHCP déjà configuré sur cette interface. Dans ce cas, l'adresse IP du VLAN est dérivée de la configuration du serveur DHCP.
Available Interface	Interfaces disponibles, pouvant être ajoutées aux autorisations pour les membres du pool. Pour placer une interface dans la liste Added Interface, cliquez sur l'interface en question, 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 en tant que membres du pont VLAN. Pour supprimer une interface de cette liste, cliquez sur l'interface en question, 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, de modifier ou d'afficher les paramètres de port.

- ÉTAPE 1** Cliquez sur **Interface Setup > LAN > Port Setting**. La fenêtre *Port Setting* s'ouvre.
- ÉTAPE 2** Indiquez les paramètres de vitesse-duplex et de contrôle du flux tels que définis dans le tableau **Paramètres de ports**. Vous pouvez configurer ces paramètres uniquement pour les ports LAN 1-4.
- ÉTAPE 3** Pour afficher les informations relatives à un port, cliquez sur un élément quelconque dans la liste Port. Les informations relatives au port s'affichent dans le tableau Port Details.
- ÉTAPE 4** Pour modifier une entrée de port, cliquez sur l'icône **Edit** (stylo). La fenêtre VLAN Port Settings s'ouvre.
- ÉTAPE 5** Indiquez les paramètres de port tels que définis dans le tableau **Paramètres de ports**.
- ÉTAPE 6** Cliquez sur **Submit** pour enregistrer les paramètres.

Paramètres de ports

Champ	Description
Mode	Décrit le comportement actuellement configuré du port. ▪ Mode Desktop : Fournit aux périphériques connectés l'accès à un VLAN données unique pour lequel la SRP fournit des services DHCP. Le trafic entrant provenant de l'hôte peut être marqué ou non marqué. Le trafic sortant vers l'hôte est non marqué. ▪ Mode IP Phone + Desktop : Le port est configuré avec un VLAN données pour l'accès natif et un VLAN voix pour l'utilisation avec un téléphone IP connecté. CDP est utilisé pour communiquer les informations du VLAN voix au téléphone.

Paramètres de ports

Champ	Description
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 trop rapidement pour que d'autres parties du réseau (y compris la station de réception) puissent les accepter. L'élément de réseau submergé envoie une trame PAUSE, qui suspend la transmission de l'expéditeur pendant une durée spécifique. Cochez cette case pour activer cette fonctionnalité. Le paramètre par défaut est Disabled.
Speed Duplex	Choisissez le mode duplex. Vous avez le choix entre Auto-negotiate, 10 Half, 10 Full, 100 Half et 100 Full. La valeur par défaut est Auto-negotiate.
Port Details	Affiche des informations détaillées sur les ports.

Configuration du LAN sans fil

Cette section décrit comment configurer les paramètres du LAN sans fil pour la SRP. Il comprend les sections suivantes :

- [Page Basic Wireless Settings](#)
- [Page Wi-Fi Protected Setup](#)
- [Page Wireless MAC](#)
- [Page Advanced Wireless Settings](#)
- [Page WMM 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 SRP et jusqu'à quatre réseaux sans fil.

La page Basic Wireless Settings permet de configurer le point d'accès sans fil intégré à 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 du réseau sans fil tels que définis dans le tableau **Paramètres sans fil de base**. Lorsque vous avez terminé, cliquez sur **Submit** pour enregistrer vos paramètres.
- ÉTAPE 3** Configurez les paramètres de sécurité réseau pour chaque SSID. Dans la zone Wireless Table, cliquez sur le lien **Edit** dans la colonne Security. La fenêtre Wireless Security s'ouvre.
- ÉTAPE 4** Choisissez le paramètre du mode de sécurité dans la liste déroulante. La valeur par défaut est Disabled.

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

Vous revenez à la page Basic Wireless.

Paramètres sans fil de base	
Champ	Description
Network Mode	Dans cette liste déroulante, sélectionnez le mode sans fil en fonction des types de périphériques 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. - Si vous disposez de périphériques sans fil-N, sans fil-G et sans fil-B dans votre réseau, sélectionnez Mixed. - Si vous avez uniquement des périphériques sans fil-G et sans fil-B dans votre réseau, sélectionnez BG-Mixed. - Si vous avez uniquement des périphériques sans fil-N, sélectionnez Wireless-N Only. - Si vous avez uniquement des périphériques sans fil-G, sélectionnez Wireless-G Only. - Si vous avez uniquement des périphériques sans fil-B, sélectionnez Wireless-B Only. - Si vous ne voulez pas utiliser le point d'accès sans fil intégré, sélectionnez Disabled.
Radio Band	Dans cette liste déroulante, sélectionnez la bande passante sans fil pour votre réseau. Trois options sont disponibles : Auto, Standard-20MHz Channel et Wide-40MHz Channel. L'option par défaut est Standard-20MHz Channel. La configuration de canal large bande est disponible pour les clients et les réseaux sans fil-N uniquement. Si le mode Wide Channel est sélectionné pour les réseaux mixtes, le mode Standard Channel est toujours disponible pour les clients sans fil-B et -G.
Wide Channel	Si vous avez sélectionné Wide-40MHz Channel pour le paramètre Radio Band, ce paramètre est alors disponible pour votre canal sans fil-N principal. Sélectionnez n'importe quel canal dans la liste déroulante. Si la bande radio est sélectionnée automatiquement, le canal à large bande est également sélectionné automatiquement.

Paramètres sans fil de base	
Champ	Description
Standard Channel	Si vous avez sélectionné Wide-40MHz Channel ou Standard - 20MHz Channel pour le paramètre Radio Band, ce paramètre est alors 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 Channel pour le paramètre Radio Band, le canal standard est un canal auxiliaire pour le réseau sans fil-N. La valeur par défaut est le canal 11. Si la bande radio est sélectionnée automatiquement, c'est le cas également pour le canal standard.
Wireless Table	
Wireless Network Name (SSID)	Nom du réseau que les clients utilisent en se connectant 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 du réseau sans fil unique, sensible à la casse et ne devant pas dépasser 32 caractères (utilisez n'importe quels caractères du clavier). Le deuxième réseau sans fil par défaut s'appelle « cisco-voice » et est relié au VLAN voix. Pour créer un deuxième 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 ITSP est peut-être chargé du contrôle des paramètres SSID2. Contactez votre ISP ou ITSP pour obtenir plus d'informations.
SSID1/2/3/4	Le SSID est le nom de réseau que partagent tous les périphériques d'un réseau sans fil donné. La SRP peut prendre en charge jusqu'à quatre réseaux sans fil. Par défaut, le premier et le deuxième réseau sans fil sont activés, et vous pouvez en activer deux autres, si nécessaire. Pour chaque réseau sans fil, vous devez configurer l'option Wireless Network Name (SSID), Broadcast Network Name et Enable Network.

Paramètres sans fil de base	
Champ	Description
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. Si vous souhaitez diffuser le SSID, laissez cette case cochée. Si vous ne souhaitez pas diffuser le SSID, décochez cette case. Dans ce cas, les utilisateurs sans fil doivent 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.

Champ	Description
Wireless Security Settings (pour y accéder, cliquez sur le bouton Edit Security d'un SSID quelconque configuré)	
Security Mode	Sélectionnez la méthode de sécurité pour votre réseau sans fil. La SRP prend en charge les options de mode de sécurité sans fil suivantes : 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). Si vous ne voulez pas utiliser la sécurité sans fil, conservez la valeur par défaut, Disabled. Cisco recommande d'utiliser le niveau de sécurité le plus élevé pris en charge par vos périphériques clients sans fil.
WEP Security Mode Settings	
WEP	WEP est une méthode de cryptage de base, qui n'est pas aussi sûre que WPA. Cette méthode peut être requise si vos périphériques réseau ne prennent pas en charge WPA.
Authentication Type	Choisissez Auto ou Shared Key. 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 sur cette page.

Champ	Description
Encryption	Sélectionnez un niveau de cryptage WEP : 64 bits (10 chiffres hexadécimaux) ou 128 bits (26 chiffres hexadécimaux). La valeur par défaut est 64 bits, 10 chiffres hexadécimaux. Des niveaux plus élevés 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 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 avez choisi le cryptage WEP de 64 bits, la clé doit contenir exactement 5 caractères ASCII ou 10 caractères hexadécimaux. Si vous choisissez le cryptage WEP de 128 bits, la clé doit contenir exactement 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 WEP, ils doivent partager la même clé.
TX Key	Sélectionnez la clé de transmission à utiliser. La valeur par défaut est 1.
WPA Personal Mode Settings	
WPA Personal	WPA Personal offre une sécurité sans fil accrue avec le cryptage avancé (TKIP ou AES).
WPA Algorithms	WPA 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 TKIP.
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 3600 secondes (1 heure).
WPA2 Personal Mode Settings	
WPA2 Personal	Fournit une sécurité sans fil accrue avec le cryptage avancé (AES ou TKIP + AES).

Champ	Description
WPA Algorithms	WPA2 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 TKIP + 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 3600 secondes (1 heure).
WPA and WPA2 Enterprise Settings	
WPA Enterprise	Cette option propose le mode WPA utilisé conjointement avec un serveur RADIUS accessible. Si vous avez deux serveurs RADIUS, sélectionnez-en un comme serveur principal, puis indiquez un serveur secondaire à utiliser en tant que serveur de sauvegarde.
WPA2 Enterprise	Cette option propose le mode WPA2 utilisé conjointement 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 le type d'algorithme (AES ou TKIP). La valeur par défaut pour WPA est TKIP. La valeur par défaut pour WPA2 est AES.
Primary RADIUS Server	▪ RADIUS Server : saisissez l'adresse IP du serveur RADIUS. ▪ RADIUS Port : saisissez le numéro de port du serveur RADIUS. La valeur par défaut est 1812. ▪ Shared Secret : saisissez la clé partagée entre la SRP et le serveur. Cette clé peut comporter entre 8 et 63 caractères ASCII ou 64 caractères hexadécimaux.
Secondary RADIUS Server	▪ RADIUS Server Address : saisissez l'adresse IP du serveur RADIUS. ▪ RADIUS Port : saisissez le numéro de port du serveur RADIUS. ▪ Shared Secret : saisissez la clé partagée entre la SRP et le serveur. Cette clé peut comporter entre 8 et 63 caractères ASCII ou 64 caractères hexadécimaux.

Champ	Description
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 3600 secondes (1 heure).

Champ	Description
Wireless Security Settings (pour y accéder, cliquez sur le bouton Edit Security d'un SSID quelconque configuré)	
Security Mode	Sélectionnez la méthode de sécurité pour votre réseau sans fil. La SRP prend en charge les options de mode de sécurité sans fil suivantes : 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). Si vous ne voulez pas utiliser la sécurité sans fil, conservez la valeur par défaut, Disabled. Cisco recommande d'utiliser le niveau de sécurité le plus élevé pris en charge par vos périphériques clients sans fil.
WEP Security Mode Settings	
WEP	WEP est une méthode de cryptage de base, qui n'est pas aussi sûre que WPA. Cette méthode peut être requise si vos périphériques réseau ne prennent pas en charge WPA.
Authentication Type	Choisissez Auto ou Shared Key. 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 sur cette page.
Encryption	Sélectionnez un niveau de cryptage WEP : 64 bits (10 chiffres hexadécimaux) ou 128 bits (26 chiffres hexadécimaux). La valeur par défaut est 64 bits, 10 chiffres hexadécimaux. Des niveaux plus élevés de cryptage offrent des niveaux accrus de sécurité, mais en raison de la complexité du cryptage, ils peuvent réduire les performances réseau.

Champ	Description
Passphrase	Saisissez un mot de passe pour générer automatiquement les clés WEP. Cliquez ensuite sur 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 avez choisi le cryptage WEP de 64 bits, la clé doit contenir exactement 5 caractères ASCII ou 10 caractères hexadécimaux. Si vous choisissez le cryptage WEP de 128 bits, la clé doit contenir exactement 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 WEP, ils doivent partager la même clé.
TX Key	Sélectionnez la clé de transmission à utiliser. La valeur par défaut est 1.
WPA Personal Mode Settings	
WPA Personal	WPA Personal offre une sécurité sans fil accrue avec le cryptage avancé (TKIP ou AES).
WPA Algorithms	WPA 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 TKIP.
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 3600 secondes (1 heure).
WPA2 Personal Mode Settings	
WPA2 Personal	Fournit une sécurité sans fil accrue avec le cryptage avancé (AES ou TKIP + AES).
WPA Algorithms	WPA2 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 TKIP + AES.

Champ	Description
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 3600 secondes (1 heure).
WPA and WPA2 Enterprise Settings	
WPA Enterprise	Cette option propose le mode WPA utilisé conjointement avec un serveur RADIUS accessible. Si vous avez deux serveurs RADIUS, sélectionnez-en un comme serveur principal, puis indiquez un serveur secondaire à utiliser en tant que serveur de sauvegarde.
WPA2 Enterprise	Cette option propose le mode WPA2 utilisé conjointement 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 le type d'algorithme (AES ou TKIP). La valeur par défaut pour WPA est TKIP. La valeur par défaut pour WPA2 est AES.
Primary RADIUS Server	▪ RADIUS Server : saisissez l'adresse IP du serveur RADIUS. ▪ RADIUS Port : saisissez le numéro de port du serveur RADIUS. La valeur par défaut est 1812. ▪ Shared Secret : saisissez la clé partagée entre la SRP et le serveur. Cette clé peut comporter entre 8 et 63 caractères ASCII ou 64 caractères hexadécimaux.
Secondary RADIUS Server	▪ RADIUS Server Address : saisissez l'adresse IP du serveur RADIUS. ▪ RADIUS Port : saisissez le numéro de port du serveur RADIUS. ▪ Shared Secret : saisissez 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 3600 secondes (1 heure).

Page Wi-Fi Protected Setup

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

REMARQUE Assurez-vous que le périphérique client WPS est situé à proximité de la SRP au moment 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 WPS pour un SSID individuel, 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.

ÉTAPE 3 WPS est activée par défaut. Sélectionnez **Disabled** if pour ne pas utiliser cette fonctionnalité pour le VLAN sélectionné.

ÉTAPE 4 Sélectionnez une méthode de configuration protégée par Wi-Fi. L'état actuel de l'accès protégé par Wi-Fi s'affiche en bas de la page.

Il existe trois méthodes pour configurer les paramètres WiFi à l'aide de WPS. Utilisez la méthode qui s'applique au périphérique client que vous avez configuré.

Méthode WPS 1

Utilisez cette méthode si le périphérique client dispose d'un bouton Wi-Fi Protected Setup.

ÉTAPE 1 Cliquez ou appuyez sur le bouton **Wi-Fi Protected Setup** sur le périphérique client, ou appuyez sur le bouton Wi-Fi protected Setup sur la façade avant de la SRP540, si elle est associée au SSID actuellement sélectionné. Reportez-vous à la section **Page Basic Wireless Settings, page 59**.

ÉTAPE 2 Cliquez sur le bouton **Wi-Fi Protected Setup** sur cette page.

ÉTAPE 3 Une fois que le périphérique client est configuré, cliquez sur OK. Reportez-vous ensuite au périphérique client ou à sa documentation pour obtenir plus d'instructions.

Méthode WPS 2

Utilisez cette méthode si le périphérique client dispose d'un code PIN Wi-Fi Protected Setup.

ÉTAPE 1 Entrez le code PIN dans le champ de cette page.

ÉTAPE 2 Cliquez sur Register.

ÉTAPE 3 Une fois que le périphérique client est configuré, cliquez sur OK. Reportez-vous ensuite au périphérique client ou à sa documentation pour obtenir plus d'instructions.

Méthode WPS 3

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

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

ÉTAPE 2 Une fois que le périphérique client est configuré, cliquez sur OK. Reportez-vous ensuite au périphérique client ou à sa documentation pour obtenir plus d'instructions.

Page Wireless MAC

La page Wireless MAC filter permet de spécifier les adresses MAC des périphériques sans fils 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 paramètre de SSID données par défaut est cisco-data et le paramètre de SSID voix par défaut est cisco-voice.

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

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

ÉTAPE 5 Si l'option Wireless MAC Filter est activée, vous pouvez cliquer 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, interface, 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.

Wireless MAC Filter Settings	
Champ	Description
Wireless MAC Filter	
Select a SSID	Choisissez le nom du réseau sans fil que vous voulez configurer. Le paramètre de SSID données par défaut est cisco-data et le paramètre de SSID voix par défaut est cisco-voice.
Enabled/Disabled	Pour filtrer les utilisateurs sans fil par adresse MAC (pour autoriser ou bloquer l'accès), sélectionnez Enabled . La valeur par défaut est Disabled.
Access Restriction (Restriction d'accès)	
Prevent	Sélectionnez cette option pour bloquer l'accès sans fil aux clients que vous avez spécifiés dans la table d'adresses MAC. Il s'agit du paramètre par défaut.
Permit	Sélectionnez cette option pour autoriser l'accès sans fil uniquement aux clients que vous avez spécifiés dans la table d'adresses MAC.
Show Client List	Cliquez sur ce bouton pour afficher la liste des ordinateurs et des autres périphériques connectés à ce réseau sans fil. Pour ajouter un client répertorié dans la table d'adresses MAC, 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 Advanced Wireless Settings permet de configurer les fonctions sans fil avancées pour la SRP.

REMARQUE Ces paramètres doivent être configurés par un administrateur expérimenté uniquement. Avant de configurer ces paramètres, assurez-vous que le mode sans fil est activé sur la SRP. Reportez-vous à la section **Page Basic Wireless Settings, page 59**.

- ÉTAPE 1** Cliquez sur **Interface Setup > Wi-Fi Settings > Advanced Wireless Settings**. La fenêtre *Advanced Wireless Settings* 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, effectuez uniquement de légères diminutions. Il est recommandé d'indiquer la valeur par défaut de 2347.
- ÉTAPE 4** Modifiez les paramètres de la zone Global Settings tels que définis dans le tableau **Paramètres sans fil avancés**.

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

Paramètres sans fil avancés	
Champ	Description
Advanced Wireless Setup	
Select a SSID	Choisissez le nom du réseau sans fil que vous voulez 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 à une station de réception 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 modifier ce seuil. Seule une légère diminution 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 2347.

Paramètres sans fil avancés	
Champ	Description
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 . Le champ AP Isolation est désactivé par défaut.
Basic Rate	Série de taux auxquels la SRP peut transmettre des données. La SRP publie son taux de base aux autres périphériques sans fil de votre réseau afin qu'ils connaissent les taux appliqués et sélectionnent automatiquement le meilleur taux de transmission. Le paramètre par défaut est Default, ce qui permet à la SRP de prendre en charge tous les taux 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 l'utilisation avec des technologies sans fil plus anciennes) et All (pour permettre à la SRP de prendre en charge tous les taux pour la transmission sans fil de données). Le paramètre Basic Rate n'indique pas le taux réel de transmission des données. Pour préciser le taux de transmission des données de la SRP, configurez le paramètre Transmission Rate.
N Transmission Rate	Vous devez définir le taux de transmission des données en fonction de la vitesse de votre réseau sans fil N. Choisissez l'une des vitesses de transmission proposées ou sélectionnez l'option Auto pour demander à la SRP d'adopter automatiquement le taux de transmission le plus rapide possible et activer la fonctionnalité de négociation automatique du débit. Cette dernière détermine la meilleure vitesse de connexion possible entre la SRP et un client sans fil. La méthode par défaut est Auto.

Paramètres sans fil avancés	
Champ	Description
Transmission Rate	Vous devez définir le taux de transmission des données en fonction de la vitesse de votre réseau sans fil. Choisissez l'une des vitesses de transmission proposées ou sélectionnez l'option Auto pour demander à la SRP d'adopter automatiquement le taux de transmission le plus rapide possible et activer la fonctionnalité de négociation automatique du débit. Cette dernière détermine la meilleure vitesse 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 méthode par défaut est Auto.
DTIM Interval	Cette valeur (entre 1 et 255) indique l'intervalle du message 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 des messages de diffusion ou de multidiffusion. Après avoir mis en mémoire tampon les messages de diffusion ou de multidiffusion des clients qui lui sont associés, la SRP transmet le DTIM suivant 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 valeur par défaut est 1.
Fragmentation Threshold	Cette valeur permet de définir la taille maximale d'un paquet avant de fragmenter les 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	
Champ	Description
Beacon Interval	Saisissez une valeur comprise entre 40 et 3500 millisecondes. L'intervalle de balise indique l'intervalle de fréquence de la balise. Une balise est un paquet diffusé par la SRP pour synchroniser le réseau sans fil. La valeur par défaut est 100.
Power Control	Sélectionnez high, middle ou low pour spécifier la plage du réseau sans fil. La valeur par défaut est high, ce qui est un niveau de puissance normal.

Page WMM Setting

La page WMM Setting permet de configurer la prise en charge de 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**. La valeur par défaut est Disabled.
- ÉTAPE 3** Pour l'option No Acknowledgement, sélectionnez **Enabled** pour désactiver la fonctionnalité d'accusé de réception, de sorte 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.

ÉTAPE 2 Pour modifier une entrée de la liste des interfaces de bouclage, cliquez sur l'icône **Edit** (stylo).

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.

Configuration du réseau

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

- [Page Routing](#)
- [Page NAT](#)
- [Page Port Range Triggering](#)
- [Page Firewall](#)
- [Page PPPoE Relay](#)
- [Page DDNS](#)
- [Page IGMP](#)
- [Page UPnP](#)
- [Page CDP Setting](#)

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

Page Routing

Cette section décrit comment configurer les différents types de routage sur le SRP, notamment :

- [Page Static Routes](#)
- [Page RIP](#)
- [Page Intervlan Routing](#)

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

Page Static Routes

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

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

À partir de cette page, vous pouvez afficher la liste de routage statique actuelle et les détails de la route sélectionnée. Vous pouvez également choisir d'ajouter une autre route à la liste de routage statique.

ÉTAPE 2 Pour ajouter une route statique, cliquez sur **Add Entry**.

La fenêtre Static Routing pour la nouvelle entrée s'ouvre.

ÉTAPE 3 Entrez un nom pour la nouvelle route.

ÉTAPE 4 Entrez l'adresse IP et le masque de sous-réseau de destination pour le réseau ou l'hôte spécifié, auquel vous souhaitez attribuer une route statique.

ÉTAPE 5 Entrez l'adresse IP de la passerelle qui permet le contact entre le SRP et le réseau ou l'hôte spécifié.

ÉTAPE 6 Choisissez l'interface pour cette route.

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

Paramètres du routage statique	
Champ	Description
Enter Route Name	Entrez un nom pour la route statique.
Destination Subnet	Adresse IP du réseau ou de l'hôte auquel vous souhaitez attribuer une route statique.
Subnet Mask	Indique quelle partie d'une adresse IP correspond à la partie réseau et quelle partie correspond à la partie hôte.
Gateway	Entrez l'adresse IP du périphérique passerelle qui permet le contact entre le 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).

Page RIP

Utilisez les pages Routing Information Protocol (RIP, Protocole d'informations de routage) pour configurer le routage dynamique sur le SRP. Vous pouvez autoriser ce protocole pour permettre aux interfaces spécifiées de s'ajuster automatiquement aux modifications physiques apportées à la présentation réseau et d'échanger les tables de routage avec celles de l'autre routeur. Le SRP détermine la route des paquets du réseau en sélectionnant le plus petit nombre d'étapes entre la source et la destination.

-
- ÉTAPE 1** Cliquez sur **Network Setup > Routing > RIP**. La fenêtre *RIP* s'ouvre.
- ÉTAPE 2** Pour activer le RIP (routage dynamique), sélectionnez **Enabled**. La valeur par défaut est Disabled.
- ÉTAPE 3** Si le RIP est activé, sélectionnez la version du RIP et les valeurs de temporisation, telles que définies dans le tableau des **Paramètres RIP**.
- Le SRP vous permet de définir les réseaux qui participeront au protocole de routage, soit par l'interface soit par le sous-réseau d'adresses IP.
- ÉTAPE 4** Cliquez sur **Submit** pour enregistrer les paramètres.
-

Paramètres RIP	
Champ	Description
RIP List	Interface : affiche la liste des interfaces. RIP Enabled : sélectionnez cette option pour activer ou désactiver le RIP sur l'interface. Passive Mode : lorsque l'interface est en mode passif, tous les paquets de réception sont traités comme à l'ordinaire et n'envoient aucun paquet RIP multidiffusion ou monodiffusion, sauf vers les RIP voisins. Pour sélectionner le mode passif, sélectionnez Enabled dans la fenêtre RIP Config Edit. Authentification : si vous envoyez et recevez des paquets RIP de version 2, vous pouvez sélectionner une authentification RIP sur une interface. Le SRP prend en charge deux modes d'authentification sur une interface : l'authentification par simple mot de passe et authentification MD5. REMARQUE : la version 1 du protocole RIP ne prend pas en charge l'authentification.
RIP Version	Pour limiter les types de paquets qui peuvent être transmis, sélectionnez Version 1 ou Version 2 . Vous pouvez également choisir RIP v1/v2 pour permettre la transmission des paquets de version 1 et 2.
RIP Timer	RIP utilise des minuteurs pour régler ses performances. Ils incluent un minuteur de mise à jour de routage, un minuteur de temporisation de la route et un minuteur d'annulation de routage. Update : spécifiez le débit auquel le SRP envoie des mises à jour de routage. La valeur par défaut est 30 secondes. Timeout : spécifiez le débit auquel le SRP compte recevoir des mises à jour de routage à partir de chaque routeur dans la table de routage. Si cette valeur est dépassée, le routage est déclaré injoignable. La route n'est pas supprimée de la table de routage avant expiration du minuteur d'annulation de routage. Flush : spécifiez la durée maximale pendant laquelle le SRP attendra une mise à jour avant de supprimer une route de la table de routage.
RIP By	Sélectionnez cette fonctionnalité si vous souhaitez activer le RIP par l'interface ou par le sous-réseau IP.
RIP List	Affiche les paramètres RIP pour toutes les interfaces SRP. Pour modifier les paramètres, cliquez sur l'icône Edit (stylo)

Page Intervlan Routing

La configuration des VLAN permet de contrôler la taille du domaine de diffusion et maintient le trafic local. Cependant, lorsqu'une station terminale d'un VLAN doit communiquer avec une station terminale d'un autre VLAN, la communication entre réseaux locaux virtuels est requise. Cette communication est activée par le routage entre réseaux locaux virtuels.

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

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

ÉTAPE 2 Pour activer le routage entre réseaux locaux virtuels, sélectionnez **Enabled**. Il s'agit du paramètre par défaut. Pour la désactiver, sélectionnez **Disable**.

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

Page NAT

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

- **Page NAT Setting**
- **Page Port Forwarding**
- **Page Port Range Triggering**

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

Page NAT Setting

Utilisez la page NAT Setting pour activer ou désactiver le routage NAT, qui permet au 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** Pour activer le NAT, sélectionnez **Enabled**. Il s'agit du paramètre par défaut. Pour désactiver le NAT, cliquez sur **Disabled**. Toutes les ALG sont désactivées par défaut.
- ÉTAPE 3** Cliquez sur **Submit** pour enregistrer les paramètres.
-

Page Port Forwarding

Utilisez la page Port Forwarding si vos services réseau d'hôtes réseau (applications Internet), tels que le Web, la messagerie électronique, le FTP, les vidéoconférences ou les jeux. Pour chaque service, le trafic Internet est transféré par l'application (port IP) aux serveurs internes qui hébergent ces services.

Le transfert de port permet au SRP de router les paquets envoyés à l'interface WAN, pour un port d'application ou pour une plage de ports spécifique, à un périphérique interne sur le réseau local. Par exemple, si vous disposez d'un serveur Web sur le LAN SRP, vous pouvez installer 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.

Après avoir cliqué sur **Add Entry**, vous pouvez créer une autre entrée pour un autre service réseau. Pour modifier une entrée, cliquez sur l'icône **Edit** (stylo).

REMARQUE Pour garantir un transfert du trafic correct, 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 **Configuration de l'interface > LAN > Serveur DHCP** pour réserver des adresses IP. Reportez-vous à la section **Page DHCP Server, page 52**.

-
- ÉTAPE 1** Cliquez sur **Network Setup > NAT > Port Forwarding**. La fenêtre *Port Forwarding* s'ouvre.
- ÉTAPE 2** Pour ajouter une entrée, cliquez sur **Add Entry**.
- La fenêtre *Manually Adding Port Forwarding* s'ouvre.
- ÉTAPE 3** Entrez les paramètres du transfert de port, comme définis dans le tableau des **Paramètres du transfert de port**.
- ÉTAPE 4** Cliquez sur **Submit** pour enregistrer les paramètres.

Paramètres du transfert de port	
Champ	Description
Port Forwarding Type	Sélectionnez le type de transfert de port dans la liste déroulante Sélectionnez Single Port Forwarding pour transférer le trafic d'un port spécifié sur le même port ou sur un autre port sur le serveur de destination sur le LAN. Sélectionnez Port Range Forwarding pour transférer le trafic d'une plage de ports vers les mêmes ports sur le serveur de destination sur 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, choisissez une application courante dans la liste déroulante (par exemple, Telnet ou DNS). Pour entrer une application qui n'est pas dans la liste, sélectionnez Add a new name, puis entrez le nom d'une nouvelle application.
Enter a Name	Pour le transfert de port unique, entrez le nom de la nouvelle application.
Wan Interface Name	Sélectionnez l'interface WAN à laquelle le trafic est adressé au départ.
External Port	Pour le transfert de port unique, entrez 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, entrez le numéro de port que le 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 port 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.
Protocol	Sélectionnez le(s) protocole(s) à transférer : TCP, UDP ou les deux.

Paramètres du transfert de port	
Champ	Description
IP Address	Entrez l'adresse IP du serveur local qui doit recevoir le trafic transféré.
Enabled	Cliquez sur Enabled pour activer cette règle de transfert. Le paramètre par défaut est Disabled.

Page Port Range Triggering

Utilisez la Port Range Triggering (Déclenchement d'une plage de ports) pour permettre au SRP de contrôler les données sortantes pour des numéros de port 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.

À partir de cette page, vous pouvez afficher les entrées existantes du déclenchement de ports depuis la liste du déclenchement d'une plage de ports, ainsi que les détails d'une entrée sélectionnée.

ÉTAPE 2 Pour modifier une entrée existante, cliquez sur l'icône **Edit** (stylo).

ÉTAPE 3 Pour ajouter une nouvelle entrée pour le déclenchement d'une plage de ports, cliquez sur **Add Entry**.

La fenêtre Port Range Triggering s'ouvre.

ÉTAPE 4 Entrez les paramètres pour le déclenchement d'une plage de ports, tels que défini dans le tableau des **Paramètres du déclenchement d'une plage de ports**.

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

Paramètres du déclenchement d'une plage de ports	
Champ	Description
Application Name	Entrez un nom pour identifier l'application de 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 où l'ordinateur hôte se trouve et auquel le trafic transféré sera dirigé.
Triggered Range	Entrez les numéros de port de début et de fin de la plage de ports déclenchée. Lorsqu'un client local établit une connexion sortante à un port dans cette plage, le SRP ouvre les ports qui sont spécifiés dans les champs Forwarded Range par le client de départ. Pour connaître les numéros de port adéquats, reportez-vous à la documentation de l'application Internet.
Forwarded Range	Entrez les numéros de port de début et de fin de la plage de ports transférée. Ces ports sont ouverts lorsqu'une connexion sortante est établie à l'un des ports spécifiés dans les champs Triggered Range. Pour connaître les numéros de port adéquats, reportez-vous à la documentation de l'application Internet.
Protocol	Sélectionnez un type de protocole dans la liste déroulante (TCP, UDP, ou les deux).
Enable	Cliquez sur Enable pour activer les applications que vous avez définies. Cette option est désactivée par défaut.

Page QoS

Cette section décrit comment configurer les paramètres de qualité de service (QoS) pour le 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** à partir de l'utilitaire de configuration.

Page QoS Bandwidth Control

Utilisez la page QoS Bandwidth Control (Contrôle de la bande passante QoS) pour permettre au 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 le désactiver. Le paramètre par défaut est Disabled.
- ÉTAPE 3** Pour configurer la bande passante disponible pour chaque interface physique, cliquez sur l'icône **Edit** (stylo). La fenêtre *Bandwidth Shaping Control* s'ouvre.
- ÉTAPE 4** Indiquez les valeurs de contrôle de mise en forme de la bande passante, comme définies dans le tableau des **Paramètres de contrôle de mise en forme de la bande passante**.
- ÉTAPE 5** Cliquez sur **Submit** pour enregistrer les paramètres.
-

Paramètres de contrôle de mise en forme de la bande passante	
Champ	Description
Upstream Bandwidth	Entrez la valeur maximale de la bande passante en amont disponible pour le service haut débit connecté. La valeur par défaut est de 100 000 Kbps pour les interfaces Ethernet. 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	Définit la bande passante nécessaire pour le trafic hiérarchisé strict. Le trafic de la file d'attente stricte compris dans ce taux est transmis avant celui de toute autre file d'attente.
High, Medium, Normal, Low	Spécifiez la priorité ou la pondération relative des files d'attente hiérarchisées élevées, moyennes, normales et faibles. La pondération de la file d'attente détermine la quantité relative de bande passante qu'il est assuré que le trafic de chaque file d'attente recevra pendant les périodes d'activité. La colonne de la bande passante fournit une indication de cette valeur permettant la bande passante hiérarchisée stricte. Pour régler la pondération relative des files d'attente, cliquez sur le bouton plus (+) et le bouton moins (-). En l'absence de trafic hiérarchisé strict, les données de ces files d'attente sont traitées sur une base « Round Robin » pondérée. REMARQUE Les valeurs de la bande passante de cette page indiquent le débit minimal garanti disponible par file d'attente pendant la charge. Des débits du trafic supérieurs peuvent être observés, lorsque les autres files d'attente sont sous-utilisées.

Page QoS Policy

Utilisez la page QoS Policy pour configurer les règles de classification, de file d'attente et de marquage du 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.
- ÉTAPE 2** Pour modifier une règle existante, cliquez sur l'icône **Edit** (stylo).
- ÉTAPE 3** Pour ajouter une nouvelle stratégie, cliquez sur **Add Entry**.
La fenêtre QoS Priority Setting s'ouvre.
- ÉTAPE 4** Sélectionnez la catégorie QoS dans la liste déroulante (application, adresse MAC, port Ethernet ou VLAN).
- ÉTAPE 5** Indiquez les paramètres de la stratégie pour la catégorie donnée, comme définis dans le tableau de **Paramètres de la politique QoS : Classification**.
- ÉTAPE 6** Entrez les paramètres de mise en file d'attente et de marquage QoS pour la catégorie spécifiée.
- ÉTAPE 7** Cliquez sur **Submit** pour enregistrer les paramètres.

Paramètres de la politique QoS : Classification	
Catégorie d'application	
Applications/ Name	Choisissez une application standard dans la liste déroulante. Pour entrer une application qui n'est pas dans la liste, sélectionnez Add a New Application , puis entrez le nom de la nouvelle application.
LAN	Choisissez le LAN source.
Port Range	Entrez 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. Les ports uniques peuvent être définis en entrant la même valeur pour les champs de début et de fin de gamme. Pour plus d'informations, reportez-vous à la documentation de l'application Internet.
Catégorie d'adresse MAC	
Name	Entrez un nom pour décrire cette règle.
LAN	Choisissez le LAN source.
MAC Address	Entrez l'adresse MAC du périphérique source au format suivant : xx:xx:xx:xx:xx:xx

Catégorie de port Ethernet	
Name	Entrez un nom pour le port Ethernet. Par exemple : Port Ethernet 1.
LAN	Choisissez le LAN source.
Ethernet	Choisissez le port Ethernet source.
Catégorie VLAN	
Name	Entrez le nom du port Ethernet. Par exemple : data_Lan.
VLAN	Choisissez le VLAN source.
Adresse IP	
Name	Entrez un nom pour décrire cette règle.
Destination IP	Entrez l'adresse IP ou le réseau de destination qui classifient le trafic pour cette règle.
Destination Mask	Entrez le masque pour l'adresse IP ou le réseau cible.
LAN	Choisissez le LAN source.
Paramètres de la politique QoS : Mise en file d'attente	
Priority	Choisissez la priorité de mise en file d'attente pour ce trafic : Strict, High, Medium, Normal ou Low.

Page CoS To Queue

Utilisez la page CoS To Queue pour mettre le trafic en file d'attente 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.
- ÉTAPE 2** Modifiez les paramètres de priorité pour chaque CoS VLAN, selon les besoins.
- Les valeurs de balise de priorité VLAN (CoS) (de 0 à 7) sont mappées à la file d'attente du routeur, où zéro est la valeur la plus basse et 7, la plus élevée.
- ÉTAPE 3** Choisissez un niveau de priorité dans la liste déroulante.

La priorité définit la file d'attente de transfert du trafic vers lequel la CoS donnée est mappée.

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

Page DSCP To Queue

Utilisez la page DSCP To Queue pour mettre le trafic en file d'attente en fonction de la valeur du point de code de services différenciés (DSCP) du 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.
- ÉTAPE 3** Choisissez un niveau de priorité dans la liste déroulante. La priorité définit la file d'attente de transfert du trafic vers lequel le trafic, avec le DSCP donné, est mappé. Les priorités disponibles sont Strict, High, Medium, Normal et Low.
- ÉTAPE 4** Cliquez sur **Submit** pour enregistrer les paramètres.
-

Page Firewall

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

- **Page Firewall Filter**
- **Page Internet Access Control**

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

Page Firewall Filter

Utilisez la page Firewall Filter pour activer le filtrage de la protection par pare-feu sur le SRP. Le pare-feu améliore la sécurité réseau et utilise la fonction 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** Sélectionnez **Enabled** pour activer la protection par pare-feu SPI. Le pare-feu est activé par défaut.
 - ÉTAPE 3** Indiquez les options Internet et de filtre Web, comme spécifiées dans le tableau des **Paramètres du filtre de pare-feu**.
 - ÉTAPE 4** Cliquez sur **Submit** pour enregistrer les paramètres.
-

Paramètres du filtre de pare-feu	
Champ	Description
SPI Firewall Protection	Sélectionnez Enabled pour activer la protection par pare-feu. La valeur par défaut est Enabled.
Options du filtre Internet	
Filter Anonymous Internet Requests	Empêche votre réseau d'être sondé par test Ping ou détecté par d'autres utilisateurs Internet. Il masque également 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	Cette fonctionnalité 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 activer le Filtre Internet NAT Redirection ou sur Disabled pour le désactiver.
Filter IDENT (Port 113)	Empêche le port 113 d'être analysé par les périphériques situés hors de votre réseau local. Ce filtre est activé par défaut. Sélectionnez Enabled pour filtrer le port 113 ou sur Disabled pour le désactiver.
Filter DoS Attack	Protège le SRP des attaques de déni de service.
Paramètres du filtre Web	
Proxy	L'utilisation des serveurs proxy WAN peut compromettre votre sécurité réseau. L'activation de l'accès à tout serveur proxy WAN par les blocs de filtre de proxy. Pour activer le filtrage des proxy, cochez la case. Par défaut, ce filtre est désactivé.

Java	Java est un langage de programmation pour les sites Web. Si vous filtrez Java, vous empêcherez l'accès aux sites Internet créés à l'aide de ce langage de programmation. Pour activer le filtrage java, cochez la case. Par défaut, ce filtre est désactivé.
ActiveX	ActiveX est un langage de programmation pour sites Web. Si vous filtrez ActiveX, vous empêcherez l'accès aux sites Internet utilisant ce langage de programmation. Pour activer le filtrage ActiveX, cochez la case. 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. 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, il est défini sur 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.
- Dans cette fenêtre, vous pouvez afficher les détails des stratégies existantes, modifier une stratégie et ajouter une nouvelle stratégie.
- ÉTAPE 2** Pour ajouter une stratégie d'accès à Internet, cliquez sur **Add Entry**. La fenêtre *Internet Access Control settings* pour que la nouvelle stratégie s'ouvre.
- ÉTAPE 3** Entrez un nom pour la stratégie d'accès à Internet.
- ÉTAPE 4** Cliquez sur **Enabled** pour activer le contrôle d'accès à Internet.
- ÉTAPE 5** Vous pouvez également choisir de cliquer sur **Show Edit List** pour afficher l'adresse MAC, l'adresse IP et les stratégies de plage d'adresses IP.
- ÉTAPE 6** Dans la zone Schedule, sélectionnez les jours et les heures pendant lesquels vous souhaitez que cette stratégie soit mise en application.
- ÉTAPE 7** Sélectionnez les autres options de blocage, selon les besoins.
- ÉTAPE 8** Cliquez sur **Submit** pour enregistrer les paramètres.
-

Paramètres du contrôle de l'accès Internet	
Champ	Description
Enter Policy Name	Entrez un nom pour la stratégie.
Status	Pour activer cette stratégie, cliquez sur Enabled . Pour désactiver cette stratégie, cliquez sur Disabled . Le paramètre par défaut est Disabled.
From, To	Vous pouvez appliquer la règle à tout le trafic en sélectionnant From All, To All ou vous pouvez limiter la règle, de sorte qu'elle s'applique uniquement à des interfaces spécifiques, telles que From VLAN1 to WAN1.
Applied PCs (Optional)	Pour appliquer la stratégie uniquement à des PC spécifiés, cliquez sur le bouton Show Edit List . Spécifiez ensuite les différents PC en entrant l'adresse MAC ou l'adresse IP. Vous pouvez spécifier les 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 mise en application. 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.
Times	Sélectionnez les heures pendant lesquelles vous souhaitez que cette stratégie soit mise en application. 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 sur cette page. Décochez cette case pour choisir une ou plusieurs 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. Entrez 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. Entrez 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). À partir de liste d'applications, cliquez sur l'application que vous souhaitez bloquer. Cliquez ensuite sur le bouton Flèche droite (>>) pour déplacer l'application vers la liste des applications bloquées. Pour Retrait d'une application de la liste des applications bloquées, cliquez dessus, puis cliquez sur le bouton Flèche gauche (<<).
Modify Application	Si l'application que vous souhaitez bloquer n'est pas répertoriée ou si vous souhaitez modifier les paramètres d'un service, entrez le nom de l'application dans le champ Application Name. Entrez la 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 Modify. Pour supprimer un service, sélectionnez-le dans la liste des applications. Cliquez ensuite sur l'icône Delete (stylo).

Page PPPoE Relay

Utilisez la page PPPoE Relay pour définir les paramètres de relais PPPoE. La fonction de relais PPPoE écoute le trafic PPP sur les interfaces LAN désignées et les transfèrent 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.
- À partir de cette page, vous ajoutez un affichage ou modifiez un relais et ajoutez 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**.
- ÉTAPE 4** Sélectionnez le WAN et les interfaces LAN pour cette règle.
- ÉTAPE 5** Cliquez sur **Submit** pour enregistrer les paramètres.

Paramètres de relais PPPoE	
Champ	Description
WAN interface	Sélectionnez l'interface WAN pour cette règle. Par exemple : WAN1 ou WAN2.
LAN interface	Sélectionnez l'interface LAN pour cette règle. Par exemple : VLAN1 ou VLAN100.
PPPoE Relay Status	Permet à un concentrateur d'accès (LAC) L2TP de relayer la fonctionnalité de détection et de sélection actives de services pour PPP over Ethernet (PPPoE) sur un canal de contrôle de protocole de tunnellation couche 2 (L2TP) vers un commutateur de serveur réseau (LNS) L2TP ou de tunnel (nœud à alimentation multiple). La fonctionnalité de relais de cette fonction permet au commutateur LNS ou au tunnel de diffuser les services qu'il offre au client, offrant ainsi un contrôle des services de bout en bout entre le LNS et un client PPPoE.

Page DDNS

Utilisez la page DNS dynamique (DDNS) pour spécifier un service Internet autorisant la localisation des routeurs avec des adresses IP publiques non statiques à l'aide des noms de domaines Internet. Une fois une nouvelle adresse IP attribuée, le SRP met à jour le service DDNS pour garantir que le nom de domaine qui y est associé correspond à cette nouvelle valeur, facilitant ainsi l'accès à distance.

REMARQUE Pour utiliser le DDNS, vous devez installer un compte avec un fournisseur DDNS, tel que 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. Vous pouvez choisir entre **DynDNS.org** et **TZO.com**. La fenêtre du service DDNS s'ouvre.
- ÉTAPE 3** Entrez les informations du service que vous avez choisi, comme spécifié dans le tableau des **Paramètres du service DDNS**.
- ÉTAPE 4** Cliquez sur **Submit** pour enregistrer les paramètres.

Paramètres du service DDNS	
Champ	Description
DDNS Service	Sélectionnez le fournisseur de votre service DDNS dans la liste déroulante. Vous pouvez choisir entre DynDNS.org et TZO.com. Le service DDNS est désactivé par défaut. REMARQUE Vous devez vous connecter à un compte avec l'un de ces fournisseurs avant de pouvoir utiliser ce service.
Paramètres DynDNS.org	
User Name	Entrez le nom d'utilisateur de DynDNS.org.
Password	Entrez le mot de passe de DynDNS.org.
Host Name	Entrez votre nom d'hôte. Par exemple : name.dyndns.org.
System	Sélectionnez le service DynDNS que vous utilisez. Vous pouvez choisir entre Dynamic, Static et Custom.

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

PAge DMZ

DMZ permet à un utilisateur local d'accéder à Internet en vue d'utiliser un service spécifique de vidéoconférence ou de jeux sur Internet, par exemple.

L'hébergement DMZ permet de transférer tous les ports en même temps vers un seul ordinateur. Le transfert de plages de ports est plus sécurisé, puisqu'il ouvre uniquement les ports que vous souhaitez ouvrir, tandis que la fonction DMZ hosting ouvre tous les ports d'un ordinateur pour lui permettre d'accéder à Internet.

Tout PC dont le port est en cours de transfert doit avoir sa fonction de client DHCP désactivée et doit disposer d'une nouvelle adresse IP statique puisque son adresse IP risque de changer lors de l'utilisation de la fonction DHCP.

ÉTAPE 1 Cliquez sur **Network Setup** dans l'onglet, puis cliquez sur **DMZ** dans le volet de navigation. La fenêtre *DMZ* s'ouvre.

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

À partir de cette page, vous pouvez afficher tous les DMZ existants et l'état DMZ, modifier un DMZ et ajouter un nouveau DMZ.

ÉTAPE 2 Pour autoriser la fonction d'hébergement DMZ, utilisez le paramètre par défaut, **Enabled**. Sinon, sélectionnez **Disabled**.

ÉTAPE 3 Spécifiez l'adresse IP source et l'adresse IP ou l'adresse MAC de destination.

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

Champ	Description
Status	Pour activer cette fonctionnalité, sélectionnez Enabled. Pour désactiver la fonction d'hébergement DMZ, sélectionnez Disabled.
Source IP Address	Si vous souhaitez qu'une adresse IP quelconque soit la source, sélectionnez Any IP Address. Si vous souhaitez définir une adresse IP ou une plage d'adresses IP comme source désignée, cliquez sur le second bouton radio et entrez la ou les adresses IP dans les champs fournis à cet effet.

Champ	Description
Destination	Pour spécifier l'hôte DMZ par adresse IP, sélectionnez IP Address et renseignez l'adresse IP dans le champ fourni à cet effet. Si vous souhaitez préciser l'hôte DMZ par adresse MAC, sélectionnez MAC Address et entrez l'adresse MAC dans le champ fourni à cet effet. Pour récupérer ces informations, cliquez sur le bouton DHCP Client Table.
Show DHCP Client Table	Le tableau des clients DHCP répertorie les ordinateurs et autres périphériques auxquels des adresses IP ont été attribuées par le routeur. La liste peut être triée par nom de client, interface, adresse IP, adresse MAC et temps expiré (temps restant pour l'adresse IP actuelle). Pour sélectionner un client DHCP, cliquez sur le bouton Select. Pour récupérer les informations les plus à jour.

Page IGMP

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

-
- ÉTAPE 1** Cliquez sur **Network Setup > IGMP**. La fenêtre *IGMP* s'ouvre.
- ÉTAPE 2** Pour permettre le trafic de diffusion via le 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** Cliquez sur **Submit** pour enregistrer les paramètres.
-

Champ	Description
Support IGMP Version	Sélectionnez la version que vous souhaitez utiliser dans la liste déroulante. Vous pouvez choisir entre IGMP v1 et IGMP v2 . Si vous n'êtes pas sûr de la version à sélectionner, conservez le paramètre par défaut, IGMP v2.
IGMP Proxy	Pour activer le proxy IGMP, sélectionnez Enabled . Cela permet au trafic de diffusion de traverser le SRP pour vos périphériques d'application multimédia.
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.

Page UPnP

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

-
- ÉTAPE 1** Cliquez sur **Network Setup > UPnP**. La fenêtre *UPnP* s'ouvre.
- ÉTAPE 2** Pour utiliser UPnP, utilisez le paramètre par défaut, **Enabled**.
- ÉTAPE 3** Configurez la manière dont UPnP peut être utilisé avec les fonctionnalités décrites dans le tableau des **Paramètres UPnP**.
- ÉTAPE 4** Cliquez sur **Submit** pour enregistrer les paramètres.
-

Paramètres UPnP	
Champ	Description
UPnP	Pour autoriser UPnP, conservez le paramètre par défaut, Enabled. Sinon, sélectionnez Disabled .
Allow Users to Configure	Une fois activé (par défaut), les clients locaux peuvent utiliser UPnP pour modifier la configuration et le comportement SRP. Si vous souhaitez permettre aux clients de détecter le SRP à l'aide d'UPnP, sélectionnez Disabled .
Keep UPnP Configurations After System Reboot	Lorsqu'il est activé, le SRP enregistre les modifications de configuration apportées par les clients après un redémarrage du système. La valeur par défaut est Disabled.
Allow Users to Disable Internet Access	Une fois activé, les clients locaux peuvent activer ou désactiver la connexion Internet SRP via UPnP. La valeur par défaut est Disabled.

Page CDP Setting

Utilisez la page CDP pour spécifier les paramètres de Cisco Discovery Protocol (CDP) sur votre réseau. CDP est un protocole de détection de périphériques au niveau des liens, disponible sur tous les équipements Cisco. Chaque périphérique compatible CDP envoie des messages périodiques à une adresse de multidiffusion et écoute également les 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 CDP sur certaines, toutes ou aucune des interfaces Ethernet SRP. Cisco recommande le paramètre par défaut, **Per Port**, qui active CDP sur les ports LAN uniquement.

ÉTAPE 2 Spécifiez les valeurs du minuteur CDP et la participation des ports, comme défini dans le tableau des **Paramètres CDP**.

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

Paramètres CDP

Champ	Description
CDP	Contrôlez si CDP fonctionne sur certaines, toutes ou aucune des interfaces Ethernet SRP. CDP per port est le paramètre par défaut (recommandé).
CDP Timer	Spécifiez l'intervalle auquel les paquets CDP successifs peuvent être envoyés. Vous pouvez entrer une valeur comprise entre 5 et 900 secondes. La valeur par défaut est 60 secondes.
CDP Hold Timer	Contrôlez si CDP fonctionne sur certaines, toutes ou aucune des interfaces Ethernet SRP. Entrez une valeur comprise entre 10 et 255 secondes. La valeur par défaut est de 80 secondes.
Interface List	Cochez la case Enable pour sélectionner les interfaces qui exécuteront CDP.

Configuration de la voix

Ce chapitre décrit comment configurer les paramètres et 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 :

- **Opérations de compréhension des ports voix**
- **Gestion des services d'ID de l'appelant**
- **Suppression des silences et services CNG (Comfort Noise Generation)**
- **Configuration des plans de numérotation**
- **Implémentation d'appel sécurisé**

Opérations de compréhension des ports voix

Le SRP520 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 sur Internet basés SIP. Outre les quatre ports (FXS) du combiné, le 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 du SRP.

Remarque : le port de la ligne SRP520 est une interface passive qui relie la ligne PSTN au port FXS 1 dans des conditions de défaillance. Les appels ne peuvent pas être routés dynamiquement vers cette interface dans des conditions de fonctionnement normal.



Le SRP maintient 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 le SRP utilise le protocole SIP (Session Initiation Protocol), il est compatible avec la plupart des offres des fournisseurs d'accès à Internet.

Fonctionnalités voix du SRP

Le SRP est fourni avec des ports voix programmables et riches en fonctionnalités, pouvant être personnalisés et fournis avec 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 du SRP**

Codecs pris en charge

Les ports voix du SRP prennent en charge les codecs suivants :

Codec	Description
G.711 (A-law and mu-law)	Codecs de très faible complexité qui prennent en charge les transmissions voix numérisées non compressées de 64 kbps de une à dix trames vocales de 5 ms par paquet. Ces codecs fournissent la qualité vocale à bande étroite la plus élevée et utilisent la plupart de la bande passante de n'importe quel des codecs disponibles.
G.726-32	Codec de faible complexité qui prend en charge la transmission voix numérisée compressée de 32 kbps 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. Reportez-vous à la section [Page Audio Configuration, page 193](#).

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 à distance. Vous pouvez nommer les différents codec individuellement, de sorte que le SRP puisse négocier avec succès le codec avec l'équipement à distance. Pour plus d'informations, reportez-vous à la section [Page Audio Configuration, page 193](#).

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. Le 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. Le SRP peut être invité à contacter un serveur proxy SIP dans un domaine nommé par le message SIP. Le 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. Le SRP tente de contacter la liste des hôtes dans l'ordre de leur priorité établie.

Si le SRP utilise actuellement un serveur proxy de faible priorité, il teste périodiquement un proxy de plus haute priorité afin de savoir 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. Reportez-vous à la section **Pages Line (1-2), page 178**.

Autres fonctionnalités voix du SRP

Le tableau suivant résume les autres fonctionnalités voix proposées par le 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 pour un simple 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. Reportez-vous à la section Page Regional, page 156. - Le mode télécopie permettant le trafic via un port voix est déclenché par la détection d'une tonalité CED/ CNG ou d'un événement NSE. - Le supprimeur d'écho est automatiquement désactivé pour le mode modem permettant le trafic via un port voix. - Le supprimeur d'écho est désactivé pour le mode télécopie permettant le trafic via un port voix si le paramètre FAX Disable ECAN (onglet Line 1 or 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). - Appel en attente et suppression des silences sont automatiquement désactivés pour Modem et fax Pass-Through. En outre, la transmission DTMF hors-bande est désactivée pendant le mode télécopie permettant le trafic via un port voix ou modem permettant le trafic via un port voix.
Adaptive Jitter Buffer	Le SRP peut protéger 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 pour satisfaire aux conditions évolutives du réseau. Le 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 le SRP tente de restreindre le tampon d'instabilité dans le temps, afin de réduire 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. Reportez-vous à la section Pages Line (1-2), page 178.

Fonctionnalité	Description
Secure Calls	Un utilisateur (s'il est autorisé par le prestataire de services ou l'administrateur) a l'option d'effectuer un appel sécurisé 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. Des paquets RTP sont configurés sur la page SIP. Reportez-vous à la section Page SIP, page 138 .
DTMF Relay	Le 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. Reportez-vous à la section Pages Line (1-2), page 178 .
Call Progress Tones	Les tonalités de progression d'appel du SRP sont configurables. Les tonalités de progression d'appel sont générées localement sur le 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 156 .
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.

Fonctionnalité	Description
Echo Cancellation	Un conflit d'impédance entre le téléphone et le port de la passerelle de téléphonie IP peut créer un écho rapproché. Le SRP comporte un supprimeur d'écho rapproché qui compense la correspondance d'impédance. Le SRP met également en œuvre un supprimeur 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. Reportez-vous à la section Pages Line (1-2), page 178.
Signaling Hook Flash Event	Le 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 des appels de tiers. Selon les fonctionnalités offertes par le fournisseur d'accès utilisant le contrôle des appels de tiers, les fonctionnalités ATA suivantes peuvent être désactivées pour signaler correctement un événement de crochet commutateur au commutateur logiciel : ▪ Call Waiting Service : fait référence au paramètre call waiting serv sur les pages Line) ▪ Three Way Conference Service : fait référence au paramètre three-way conf serv dans les pages Line) ▪ Three Way Call Service : fait référence au paramètre three-way call serv dans les 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. Reportez-vous à la section Page Regional, page 156.

Fonctionnalité	Description
Configurable Dial Plan with Interdigit Timers	Le SRP comporte trois minuteurs inter-chiffres configurables : ▪ Initial timeout (T) : signale que le combiné est décroché et qu'aucun chiffre n'a été encore 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 plus d'informations, reportez-vous à la section Configuration des plans de numérotation, page 119.
Polarity Control	Le 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. Reportez-vous à la section Pages Line (1-2), page 178.
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 auquel ils doivent se désengager. CPC est configuré dans la page Regional. Reportez-vous à la section Page Regional, page 156.
Report Generation and Event Logging	Le 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 de la page System. Reportez-vous à la section Page System, page 137.

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, le 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 à la section Page System, page 137.
SIP Over TLS	Le 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 à la section Pages Line (1-2), page 178.

Enregistrement auprès du prestataire de services.

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

REMARQUE Chaque onglet Line 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 la connexion administrative fournie 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 **Line** (Line 1-2) pour choisir l'interface de ligne 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.
-



REMARQUE 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 configuré correctement.
-

Gestion des services d'ID 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 (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). Il s'agit du paramètre par défaut.
DTMF (Finland, Sweden) : CID uniquement. DTMF envoyé après l'inversion de 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 (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
Le 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 1 (d) et (e)). 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 à distance a changé ou a été mise à jour (par exemple, à cause d'un transfert d'appels). Cette fonctionnalité est disponible uniquement pour les méthodes CID basées sur FSK : (Bellcore, ETSI FSK et ETSI FSK With PR).



Optimisation des taux d'aboutissement de la télécopie

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 le SRP. Vous pouvez régler plusieurs paramètres sur votre SRP pour optimiser vos taux d'aboutissement de la télécopie.

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 kbps environ.
- T.38 nécessite au moins 50 Kbits/s.

ÉTAPE 2 Afin d'optimiser le taux d'aboutissement de la télécopie de G.711 fallback, définissez ce qui suit dans l'onglet Line de votre SRP :

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

Lorsque vous utilisez une passerelle multimédia Cisco pour les terminaisons RTPC, désactivez T.38 (relais fax) et activez le fax à l'aide du modem Pass-Through. 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 le SRP en configurant les paramètres ci-dessous dans l'onglet Line du port FXS auquel le télécopieur est connecté :

```
FAX_Passthru_Method: ReINVITE
```

REMARQUE 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 réglages ci-dessous :

Assurez-vous que la passerelle Cisco est correctement configurée pour T.38 avec le terminal de numérotation dial-peer SPA. 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 périphériques ATA.

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 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&password=<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.

Suppression des silences et services CNG (Comfort Noise Generation)

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 nécessaire pour un simple 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 VAD 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 des silences et les services CNG (Comfort Noise Generation) sont activés. C'est le cas lors de la suppression de la transmission des silences naturels qui survient dans la connexion bi-directionnelle normale. Ainsi, 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.

La suppression des silences est configurée à partir des pages Line (1-2). Reportez-vous à la section **Pages Line (1-2), page 178**.

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 le caractère « | ». 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.
[sequence]	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'utilisateur à appuyer sur tout chiffre compris entre 2 et 9. - Plage numérique avec d'autres caractères : Par exemple, vous devez entrer [35-8*] pour autoriser l'utilisateur à appuyer sur les 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 zéro. Par exemple, 01. permet aux utilisateurs d'entrer 0, 01, 011, 0111 et ainsi de suite.

Séquence de chiffres	Fonction
<dialled: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 19725550112.
,	Entrez une virgule entre les chiffres pour émettre une tonalité de « ligne extérieure » après la saisie de la séquence par l'utilisateur. EXEMPLE : 9, 1xxxxxxxxxx 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.
!	Entrez un point d'exclamation pour interdire un modèle de séquence de numérotation. EXEMPLE : 1900xxxxxxxx! 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>xxxxxxxx | 9, 1 [2-9] xxxxxxxx | 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>xxxxxxxx | 9, 1 [2-9] xxxxxxxx | 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

EXEMPLE: ([1-8]xx | 9, xxxxxxx | 9, <:1>[2-9]xxxxxxxxx | 8, <:1212>xxxxxxxx | 9, 1 [2-9] xxxxxxxx | 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.

EXEMPLE: ([1-8]xx | 9, xxxxxxx | 9, <:1>[2-9]xxxxxxxxx | 8, <:1212>xxxxxxxx | 9, 1 [2-9] xxxxxxxx | 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 saisir 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.

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

9, 1 [2-9] xxxxxxxx Lorsque l'utilisateur appuie sur la touche 9, une tonalité extérieure 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]xxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9] xxxxxxxx | **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 extérieure 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]xxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9] xxxxxxxx | 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]xxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9] xxxxxxxx | 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.
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:** le nombre de secondes ; si aucun nombre n'est entré après *P*, le minuteur par défaut de 5 secondes s'applique.
- **n:** (facultatif) : le 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]xxxxxxxxxx | 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]xxxxxxxxxx | 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: (PO <:1000>)

Lorsque le temporisateur est réglé sur 0 seconde, l'appel est transmis automatiquement au poste spécifié dès que le combiné est décroché.

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. Reportez-vous à la section **Réinitialisation des temporisateurs de contrôle, page 128**.

Syntaxe du temporisateur long inter-chiffres

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

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

Exemple de temporisateur long inter-chiffres

EXEMPLE: L:15, (9,8<:1408>[2-9]xxxxxx | 9,8,1[2-9]xxxxxxxxxx | 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: le 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]xxxxxxxxxx | 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 les chiffres avant l'expiration du minuteur inter-chiffres court. .

- 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 portuse.

-
- ÉTAPE 1** Connectez-vous à l'utilitaire de configuration. Si vous y êtes invité, entrez la connexion administrative fournie 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 Line (Line 1-2) pour choisir l'interface de ligne que vous souhaitez modifier.
- ÉTAPE 3** Faites défiler l'écran jusqu'à la section *Dial Plan*.
- ÉTAPE 4** Entrez les séquences de chiffres dans le champ **Dial Plan**. Pour plus d'informations, reportez-vous à la section **À propos des plans de numérotation, page 119**.
- 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, vous pouvez modifier le plan de numérotation. Reportez-vous à la section **À propos des plans de numérotation, page 119**.

-
- ÉTAPE 1** Connectez-vous à l'utilitaire de configuration. Si vous y êtes invité, entrez la connexion administrative fournie 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 le 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 SIPINFO. Les réponses à ce message utilisent un format propriétaire. Si cette seconde étape est réussie, le 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 l'ID de l'appelant pour les appels en attente (CIDCW) et que ce service est activé, le CID est mis à jour à l'aide des informations extraites du Mini-certificat reçu du tiers à distance. 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 ensemble de manière sécurisée. La clé publique de l'agent de signature est préconfigurée dans le SRP par l'administrateur et elle est utilisée par le 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.

Le SRP peut être configuré 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.

Le 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. Le 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 de 1024 bits codées base64 pour signer/vérifier le MC. Le texte suivant en est un exemple :

```
9CC9aYU1X51JuU+EBZmi3AmcqE9U1LxEogwopaGyGOh3VyhKgi6JaVtQZt87PiJINKW8XQj3B9Qq
e3VgYxWCQNa335YCNdsenASeBxuMIEaBCYd111fVEodJZOGwXwfAde0MhcbD0kj7LVlzcS
Tyk2TZYTccnZ75TuTjj13qvYs=5nEtOrkCa84/mEwl3D9tSvVLyLiwQ+u/
Hd+C8u5SNk7hsAUZaA9TqH8Iw0J/
IqSrsf6scsmundY5j7Z5mK5J9uBxSB8t8vamFGD0pF4zhNtbrVvIXKI9kmp4vph1C5jzO9gDfs3M
F+zjyYrVUFdM+pXtDBxmM+fGUfrpAuXb7/k=
```

- **user-name** est le nom de l'abonné, par exemple « Jean Dupont ». Celle-ci peut contenir au maximum 32 caractères.
- **user-id** est l'ID 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>
Sm9lIFNtaXR0AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAxNDA4NTU1MTIzNAAAAAAAAAMDAwMDAwMDEw
MTM0O0vJakde2vVMF3Rw4pPXL7lAgIagMpbLSAG2+++YlSqt198Cp9rP/
xMGFFoPmDKGx6JFtkQ5sxLcuwgxpXpXkeXvpZKlYlpsb28L4Rhg5qZA+Gqj1hDFCmG6dffZ9Sjhx
ES767G0JIS+N8lQBLr0AuemotknSjjjOy8c+1lTCd2t44Mh0vmwNg4fDck2YdmTMBR516xJt4/
uQ/
LJQlni2kwqlm7scDv115k232EvvvVtCK0AYa4eWd6fQOpIESCO9CC9aYU1X51JuU+EBZmi3AmcqE
9U1LxEogwopaGyGOh3VyhKgi6JaVtQZt87PiJINKW8XQj3B9Qqe3VgYxWCQNa335YCNdsenASeBx
uMIEaBCYd111fVEodJZOGwXwfAde0MhcbD0kj7LVlzcS Tyk2TZYTccnZ75TuTjj13qvYs=
<SRTP Private Key>
b/DWc96X4YQraCnYzl5en1CIUhVQQqrvcR6Qd/8R52IEvJjOw/
e+Klm4XiiFEPaKmU8UbooxKG36SEdKusp0AQ==
```

Configuration des paramètres de voix

Utilisez les pages Voix 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 (1-2)**
- **Pages User (1-2)**

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 :

- **Page Product Information**
- **Page System Status**
- **Page Line Status**

Page Product Information

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 le SRP est autorisé par votre ITSP.
Serial Number	Numéro de série du produit.
Hardware Version	Numéro de version matérielle.
MAC Address	Adresse MAC. Par exemple : 8843E1657936.
Customization	Fonctionnalité non utilisée.

Page System Status

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 des messages SIP reçus (y compris les retransmissions)

Page Line Status

Voice > Info > Line 1 Status (des informations similaires ont également été fournies pour la ligne 2)

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.

Page System

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

- **Page System Configuration**
- **Page Miscellaneous Settings**

Page System Configuration

Voice > System > System Configuration

Restricted Access Domains	Fonctionnalité actuellement inutilisée par le SRP.
IVR Admin Password	Mot de passe pour que l'administrateur gère le SRP à l'aide de l'IRV 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'IRV intégré via son combiné. La valeur par défaut est no password .

Page Miscellaneous Settings

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, 3 ou 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 :

- **Page SIP Parameters**
- **Page SIP Timer Values**
- **Page Response Status Code Handling**
- **Page RTP Parameters**
- **Page SDP Payload Types**
- **Charge utile dynamique NSE**

Page SIP Parameters

Voice > SIP > SIP Parameters

Max Forward	Valeur maximale de transfert, qui peut s'étendre de 1 à 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 le 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, le SRP utilise les en-têtes SIP compacts dans les messages SIP sortants. S'il est défini sur no, le SRP utilise des en-têtes SIP normaux. Si les demandes SIP entrantes contiennent des en-têtes compacts, le 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, le 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 le 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.

Page SIP Timer Values

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–(2³¹–1).
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–(2³¹–1).
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 le 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, le SRP patiente pendant l'intervalle indiqué avant d'effectuer une nouvelle tentative. Si cet intervalle est égal à 0, le SRP interrompt ses tentatives. Cette valeur doit être supérieure à la valeur Reg Retry Intvl non nulle. La valeur par défaut est 1200
----------------------	---

Page Response Status Code Handling

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 d'occupation est émise par défaut pour tous les codes d'état d'échec de réponse de SIT 1 RSC à SIT 4 RSC.
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 le SRP n'effectue une nouvelle tentative d'enregistrement après le dernier échec.

Page RTP Parameters***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 le SRP ne mette fin à l'appel. Si la valeur est définie sur 0, le 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, le SRP peut être programmé 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. 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 Vendor/Hardware-platform-software-version (par exemple, Cisco/srp520 1.0.31(b)). L'horodatage NTP utilisé dans le SR est un instantané de l'heure locale du SRP et non de l'heure rapportée par le serveur NTP. Si le SRP reçoit un RR d'un homologue, il tente de calculer le délai du trajet et l'exprime alors comme valeur <Call Round Trip Delay> (en millisecondes) sur la page Voice > Info. La valeur par défaut est 0.
No UDP Checksum	Sélectionnez yes si vous souhaitez que le 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 le périphérique 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.

Page SDP Payload Types

Voice > SIP > SDP Payload Types

Charge utile dynamique NSE	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.
Charge utile dynamique RTP-Start-Loopback	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 NSE dans 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.

Page NAT Support Parameters

Voice > SIP > NAT Support Parameters

Handle VIA received	Si vous sélectionnez yes , le 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 , le 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, le 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 le 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 du 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, le SRP utilise cette adresse IP lorsqu'il 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 le 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 de mise en service pour configurer différents profils et paramètres. Cette page comprend les sections suivantes :

- **Page Configuration Profile**
- **Page Firmware Upgrade**
- **Page General Purpose Parameters**

Page Configuration Profile

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 mise en service 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	La valeur maximale pour un intervalle aléatoire pendant lequel le périphérique attend avant d'établir son initial contact avec le serveur de mise en service. Ce délai est efficace uniquement sur la tentative de configuration initiale, à la suite du démarrage ou de 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	L'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 de 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	Active une resynchronisation à déclencher 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 du déclencheur de 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.
Règle de profil	Ce paramètre est un script de profil qui est évalué à l'aide de la commande de resynchronisation de l'approvisionnement. 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 fonctionnalité 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 défectueuse. La valeur par défaut \$PN \$MAC – Resync failed: \$ERR.
Report Rule	L'URL de destination vers 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).

Page Firmware Upgrade***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 le SRP500.

Page General Purpose Parameters

Voice > Provisioning > General Purpose Parameters

GPP A to GPP P	Paramètres de mise en service 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 Regional.

- **Page Call ProgressTones**
- **Page Distinctive Ring Patterns**
- **Page Distinctive Call Waiting Tone Patterns**
- **Page Distinctive Ring/CWT Pattern Names**
- **Spécification de la tonalité d'appel en attente et de sonnerie**
- **Page Control Timer Values (sec)**
- **Page Vertical Service Activation Codes**
- **Page Vertical Service Announcement Codes**
- **Page Outbound Call Codec Selection Codes**
- **Page Miscellaneous**

Définition des scripts de cadence et de tonalité de la sonnerie

Pour définir la sonnerie et modifier les modèles de tonalité, le 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

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

Syntaxe : $S_1[S_2]$, où :

$S_i = D_i(\text{on}_{i,1}/\text{off}_{i,1}, \text{on}_{i,2}/\text{off}_{i,2}, \text{on}_{i,3}/\text{off}_{i,3}, \text{on}_{i,4}/\text{off}_{i,4}, \text{on}_{i,5}/\text{off}_{i,5}, \text{on}_{i,6}/\text{off}_{i,6})$ et est connu en tant que section, $\text{on}_{i,j}$ et $\text{off}_{i,j}$ 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 = 1
Cadence Section 1: Section Length = 60 s
Number of Segments = 1
Segment 1: On=2s, Off=4s
Total Ring Length = 60s
```

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

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

FreqScript

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

Syntaxe : F₁@L₁[F₂@L₂[F₃@L₃[F₄@L₄[F₅@L₅[F₆@L₆]]]]]

où F₁-F₆ représente la fréquence en Hz (entiers non signés uniquement) et L₁-L₆ sont les niveaux correspondants en dBm, avec une décimale au maximum). Les espaces blanches avant et après la virgule sont autorisées (mais non recommandées).

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

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

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

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

ToneScript

Un mini-script de 127 caractères maximum qui spécifie les paramètres de fréquence, de niveau et de cadence d'une tonalité de progression d'appel. Peut contenir jusqu'à 127 caractères.

Syntaxe : FreqScript;Z₁[:Z₂].

La section Z₁ est similaire à la section S₁ d'un CadScript, sauf que chaque segment activé ou désactivé est suivi d'un paramètre de composants de fréquence : Z₁ = D₁(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}[,on_{i,5}/off_{i,5}/f_{i,5}[,on_{i,6}/off_{i,6}/f_{i,6}]]]]]), où f_{i,j} = n₁[+n₂]+n₃[+n₄]+n₅[+n₆]]]] et 1 < n_k < 6 indique quels sont les composants de fréquence donnés dans le FreqScript utilisés dans ce segment ; si plusieurs composants de fréquence sont utilisés dans un segment, les composants sont additionnés ensemble.

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

Page Call ProgressTones***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 à distance raccroche au cours d'un appel en cours. 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 Warning Tone	Cette tonalité est émise lorsque l'appelant n'a pas correctement replacé le combiné sur son support. Le décrochage avec tonalité d'avertissement est émis 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 la partie appelée 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).

Page Distinctive Ring Patterns

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).

Page Distinctive Call Waiting Tone Patterns

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

Page Distinctive Ring/CWT Pattern Names***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.
------------	---

Spécification de la tonalité d'appel en attente et de sonnerie

IMPORTANT : la sonnerie et les tonalités d'appel en attente ne fonctionnent pas comme 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

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 le SRP est appelé, toutes les lignes sonnent en même temps (comme c'est le cas pour une PSTN standard). Lorsqu'une ligne répond, les autres arrêtent de sonner. La valeur par défaut est no.

Page Control Timer Values (sec)

Voice > Regional > Control Timer Values (sec)

Hook Flash Timer Min	Durée minimale de combiné raccroché avant que le décrochage ne soit considéré comme 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 crochet commutateur. Cette durée dépassée, l'événement combiné raccroché est traité comme tel (et non comme un événement crochet commutateur). Intervalle : De 0,4 à 1,6 secondes. La valeur par défaut est 0.9.
Callee On Hook Delay	Le combiné du téléphone doit être raccroché pendant cette durée, en secondes, avant que le 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, le 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 le SRP supprime la tension des fils de pointe et de nuque de l'équipement connecté de la partie appelée. La plage est comme suit : de 0 à 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.
CPCDuration	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).

Page Vertical Service Activation Codes

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	Code de renvoi d'appel : ce 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 envoyer un message radio à 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 au SRP quelle opération effectuer lorsque l'utilisateur place l'appel en cours en attente et écoute la deuxième tonalité. 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 de destination valide suivant selon le plan de numérotation actuel) entré lors de la deuxième tonalité déclenche la réalisation par le SRP d'un transfert aveugle vers le numéro de destination ajouté par le code * de service. Par exemple, lorsque l'utilisateur compose le code *98, le SRP émet une tonalité spéciale appelée « Tonalité d'invite » en attendant que l'utilisateur entre un numéro de destination (qui est vérifié conformément au plan de numérotation, comme lors d'une numérotation normale). Une fois le numéro complet entré, le SRP envoie un message REFER aveugle à l'interlocuteur en attente, avec la cible Refer-To correspondant à *98 target_number. Cette fonctionnalité permet au SRP de transférer l'appel à un serveur d'application afin de poursuivre le traitement, comme le parage d'appels. Les codes * ne doivent pas entrer en conflit avec les autres codes de service vertical traités en interne par le SRP. Vous pouvez supprimer le code * correspondant que vous ne souhaitez pas que le SRP traite.

Feature Dial Services Codes	Ces codes indiquent au SRP quelle opération effectuer lorsque l'utilisateur écoute la première ou la deuxième tonalité. 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). Entrez un code * (et le numéro de destination valide suivant selon le plan de numérotation actuel) entré lorsque la tonalité déclenche l'appel par le SRP du numéro de destination ajouté par le code *. Par exemple, une fois que l'utilisateur a composé *72, le 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 entré, le 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 le SRP. Vous pouvez supprimer le code * correspondant que vous ne souhaitez pas que le 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, le 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 le SRP envoie un message INVITE *73@.... comme d'habitude lorsque l'utilisateur compose *73.
--	---

Page Vertical Service Announcement Codes

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.

Page Outbound Call Codec Selection Codes

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.

Page 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.
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 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. Cette configuration n'a aucun effet si le paramètre DTMF Tx Method est configuré sur INFO ; ABCD est toujours envoyé hors bande quelle que soit cette configuration.
Playback ABCD	Sélectionnez yes pour activer la lecture locale de OOB DTMF ABCD. Sinon, sélectionnez no. La valeur par défaut est yes.

Caller ID Method	Les choix suivants sont disponibles : ▪ 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 and 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. 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	Le 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 (1-2)

Utilisez les pages Line (Line 1-2) pour configurer les lignes pour les services voix. Ces pages incluent les sections suivantes :

- **Page Line Enable**
- **Page Streaming Audio Server (SAS)**
- **Page NAT Settings**
- **Page Network Settings**
- **Page SIP Settings**
- **Page Call Feature Settings**
- **Page Proxy and Registration**
- **SIP proxy sortant**
- **Page Supplementary Service Subscription**
- **Page Audio Configuration**
- **Page Dial Plan**
- **FXS Port Polarity Configuration**

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.

Page Line Enable

Voice > Line 1–2 > Line Enable

Line Enable	Pour activer cette ligne pour le service, sélectionnez yes. Sinon, sélectionnez no. La valeur par défaut est yes.
-------------	--

Page Streaming Audio Server (SAS)

Voice > Line 1–2 > 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, le 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.
----------------------	---

Page NAT Settings

Voice > Line 1-2 > NAT Settings

NAT Mapping Enable	Pour utiliser les adresses IP et les ports SIP/RTP mappés en externe dans les messages SIP, sélectionnez yes. Sinon, sélectionnez no. La valeur par défaut est no.
--------------------	--

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.

Page Network Settings

Voice > Line 1-2 > 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 le 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 ou 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 ou disable. Le paramètre par défaut est up and down.

Page SIP Settings

Voice > Line 1-2 > 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 : TCP, UDP, 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 des 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, le 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, le 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. Les choix suivants sont disponibles : ▪ 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, le 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 le 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, le 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 du 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, le 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.

Page Call Feature Settings

Voice > Line 1-2 > Call Feature Settings

Blind Attn-Xfer Enable	Permet au SRP d'effectuer une opération de renvoi manuel d'appel en mettant fin au signal d'appel en cours et en procédant à un transfert aveugle de l'autre signal d'appel. Si cette fonctionnalité est désactivée, le SRP effectue une opération de renvoi d'appel en renvoyant l'autre signal d'appel vers le signal d'appel actuel 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@myserver.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.

Page Proxy and Registration***Voice > Line 1-2 > Proxy and Registration***

Proxy	Serveur proxy SIP pour toutes les requêtes sortantes.
SIP proxy sortant	Serveur proxy SIP sortant vers lequel toutes les demandes sortantes sont envoyées comme premier saut.
Use Outbound Proxy	Active 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) s 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 Normal ou Based on SRV Port. Le 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, le 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.

Page Subscriber Information***Voice > Line 1–2 > Subscriber Information***

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 CA avec 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.

Page Supplementary Service Subscription

Le SRP offre une prise en charge native de nombreux services optimisés 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 le SRP.

Voice > Line 1-2 > 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 MWI est 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 .

Page Audio Configuration

Voice > Line 1-2 > 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, or 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 un des éléments suivants : Unspecified, G711u, G711a, G726-16, G726-24, G726-32, G726-40, G729a, or G723. La valeur par défaut est Unspecified.
Use Pref Codec Only	Pour utiliser uniquement le codec préféré 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 kbps, sélectionnez yes. Sinon, sélectionnez no. La valeur par défaut est yes.
Echo Canc Enable	Pour activer l'utilisation du supprimeur d'écho, sélectionnez yes. Sinon, sélectionnez no. La valeur par défaut est yes.
Echo Canc Adapt Enable	Pour activer l'adaptation du supprimeur d'écho, sélectionnez yes. Sinon, sélectionnez no. La valeur par défaut est yes.

Echo Supp Enable	Pour activer l'utilisation du supprimeur 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 kbps, 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 le 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	DTMF 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 de 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 numéro 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 plus 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 : le SRP détecte la tonalité du télécopieur qu'il s'agisse de l'appelant ou de l'appelé ▪ caller only : le SRP détecte la tonalité du télécopieur uniquement s'il s'agit de l'appelant. ▪ callee only : le SRP détecte la tonalité du télécopieur uniquement s'il s'agit de l'appelé La valeur par défaut est caller or callee.

Page Dial Plan

Le script du plan de numérotation par défaut pour chaque ligne est le suivant : (*xx[3469]110|00[2-9]xxxxxx|1xxx[2-9]xxxxxx|xxxxxxxxxxxx.). La syntaxe pour une expression du plan de numérotation est décrite dans le tableau ci-dessous.

Voix > Line 1-2 > 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]xxxxxxx	Numéro local des États-Unis
1xxx[2-9]xxxxxx	Numéro longue distance avec 10 chiffres + 1 pour les États-Unis
xxxxxxxxxxxx.	Tout le reste (longue distance internationale, FWD, ...)
Dial Plan	Script du plan de numérotation pour cette ligne. La valeur par défaut est (*xx[3469]110 00[2-9]xxxxxx 1xxx[2-9]xxxxxxS0 xxxxxxxxxxxx.). Chaque paramètre est séparé par un point-virgule (;). Exemple 1 : <pre>*1xxxxxxxxxx<:@fwdnat.pulver.com:5082;uid=jsmith;pwd=xy z</pre> Exemple 2 : <pre>*1xxxxxxxxxx<:@fwd.pulver.com;nat;uid=jsmith;pwd=xyz</pre> Exemple 3 : <pre>[39]11<:@gw0></pre>
PSTN Fallback Dial Plan	Script du plan de numérotation pour router 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, 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, le SRP désactive le traitement de l'événement de 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.

FXS Port Polarity Configuration

Voice > Line 1-2 > 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.

Pages User (1–2)

Utilisez ces pages pour configurer les paramètres utilisateur. Ces pages incluent les sections suivantes :

- **Page Call Forward Settings**
- **Page Selective Call Forward Settings**
- **Page Speed Dial Settings**
- **Page Supplementary Service Settings**
- **Page Distinctive Ring Settings**
- **Page Ring Settings**

Lorsqu'un appel est effectué à partir de la ligne 1 ou de la ligne 2, le SRP utilise les paramètres de l'utilisateur et de la ligne ; il n'y a pas de prise en charge de la connexion utilisateur. [1] ou [2] (correspondant à la ligne 1 ou 2) doit être ajouté aux balises des paramètres utilisateur dans le profil de configuration. Ces caractères sont omis ci-dessous pour une meilleure lisibilité.

Page Call Forward Settings

Voice > User 1–2 > 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.

Page Selective Call Forward Settings

Voice > User 1–2 > 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	ID de 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.

Page Speed Dial Settings

Voice > User 1–2 > 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.
----------------	---

Page Supplementary Service Settings

Le SRP offre une prise en charge native de nombreux services optimisés 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 le SRP.

Voice > User 1-2 > 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	Génération 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 d'abord, 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. REMARQUE Si le 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. Notez que si le périphérique SRP répond à l'appel, le type de bouclage est alors choisi par l'appelant (le SRP choisit toujours le premier type de bouclage si l'offre en contient plusieurs).

Page Distinctive Ring Settings

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 1-2 > 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.
------------------	---

Page Ring Settings

Voice > User 1-2 > 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.

La configuration VPN

Ce chapitre décrit comment configurer les stratégies VPN et les paramètres pour le SRP. Il comprend les sections suivantes :

- [Page IKE Policy](#)
- [Page IPsec Policy](#)
- [Page GRE Tunnel](#)
- [Page VPN Passthrough](#)
- [Page Serveur Cisco VPN](#)

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

Page IKE Policy

Utilisez la page IKE Policy pour configurer une stratégie IKE VPN. Chaque stratégie IKE contient les paramètres pour définir des règles d'authentification IKE. Ces stratégies IKE sont utilisées dans différentes stratégies VPN

ÉTAPE 1 Cliquez sur **VPN > Site to Site IPsec VPN > IKE Policy**. La fenêtre *IKE Policies* s'ouvre.

Dans cette fenêtre, vous pouvez afficher les stratégies IKE existantes à partir de la liste des stratégies IKE, modifier une stratégie, afficher les détails des stratégies et ajouter une nouvelle stratégie IKE.

ÉTAPE 2 Pour ajouter une stratégie IKE, cliquez sur **Add Entry**. La fenêtre IKE Policy configuration pour la nouvelle stratégie s'ouvre.

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. Vous pouvez choisir le mode **Main** ou **Aggressive**.

Sélectionnez le mode principal pour une sécurité plus élevée, mais avec une connexion plus lente. Sélectionnez le mode agressif pour une connexion plus rapide, mais avec une sécurité réduite.

- ÉTAPE 5** Définissez les paramètres IKE SA comme nécessaire et tels que définis dans le tableau des **Paramètres des stratégies IKE**.
- ÉTAPE 6** Si vous êtes connecté à un serveur XAUTH, entrez un nom d'utilisateur et un mot de passe. Lorsqu'il est activé, le SRP peut authentifier les utilisateurs d'un serveur d'authentification externe, comme un serveur RADIUS.
- ÉTAPE 7** Cliquez sur **Submit** pour enregistrer les paramètres.

Paramètres des stratégies IKE	
Champ	Description
Généralités	
Policy Name	Entrez un nom unique pour la stratégie VPN.
Exchange Mode	Choisissez le mode d'échange en fonction de vos exigences de sécurité et vitesse. ▪ Main : sélectionnez ce mode pour une sécurité plus élevée, mais avec une connexion plus lente. 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 : choisissez ce mode si vous souhaitez une connexion plus rapide, mais avec une sécurité réduite. En mode agressif, les échanges de clés entre l'initiateur et le destinataire sont moins nombreux. Les deux côtés échangent des informations, même avant qu'un canal sécurisé n'existe.
Paramètres IKE SA	
Encryption Algorithm	Sélectionnez un mode de cryptage. Sélectionnez entre DES , 3DES , AES128 , AES192 et AES256 .
Authentication Algorithm	Choisissez un algorithme d'authentification pour IKA SA. Choisissez entre MD5 et SHA1 .
Pre Shared Key	Entrez une clé alphanumérique à partager avec l'homologue IKE.

Paramètres des stratégies IKE	
Champ	Description
Diffie-Hellman (DH) Group	Sélectionnez un groupe DH afin de définir la puissance de l'algorithme, en bits. Sélectionnez entre Group 1 (768 bits) et Group 2 (1024 bits) .
Enable Dead Peer (DPD) Detection	Pour activer la DPD, sélectionnez Enable . Cette option est désactivée par défaut. REMARQUE La DPD n'est pas requise pour une règle IKE, mais si cette fonction est activée, elle permet de préserver la connexion active pendant les périodes sans trafic.
Intervalle DPD	Entrez un intervalle pour la DPD. Ce paquet est régulièrement envoyé, en secondes pendant l'intervalle, en l'absence de trafic de données.
DPD Timeout	Entrez un délai d'expiration (en secondes) pour DPD.
Authentification étendue	
XAUTH Client Enable	Activez cette fonctionnalité si l'homologue VPN exige des informations d'identification de l'authentification étendue. Le paramètre par défaut est disabled.
Nom d'utilisateur/mot de passe	Entrez les informations d'identification que le SRP utilise pour se connecter à l'homologue à distance.

Page IPSec Policy

Utilisez la page IPSec Policy pour configurer une stratégie IPSec VPN. La stratégie VPN IPSec contient les paramètres IPSec Security Association, 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 et ajouter une stratégie IPSec. Vous pouvez également afficher les informations détaillées de chaque stratégie dans la liste des détails IPSec.

ÉTAPE 2 Pour ajouter une stratégie IPSec, cliquez sur **Add Entry**. La 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 liste déroulante.
- 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. Vous pouvez choisir entre **Auto** et **Manual**.
- ÉTAPE 7** Entrez les paramètres de stratégie IPSec comme définis dans le tableau des **Paramètres des stratégies IPSec**.
- ÉTAPE 8** Cliquez sur **Submit** pour enregistrer les paramètres.

La stratégie VPN apparaît dans la liste des stratégies IKE sur la page Add Entry de la stratégie IKE.

Paramètres des stratégies IPSec	
Paramètres généraux	
Policy Name	Entrez un nom unique pour la stratégie VPN.
Policy Type	Sélectionnez le type de stratégie. Sélectionnez entre Auto Policy et 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 > de la stratégie IKE. La stratégie manuelle n'utilise pas IKE, ce qui la rend plus simple, mais moins sécurisée.
Remote Endpoint	Choisissez la manière dont vous souhaitez identifier la passerelle à distance 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). Soyez conscient qu'un FQDN exige que le SRP puisse se connecter à un serveur DNS pour résoudre l'adresse avant d'établir le tunnel VPN.

Paramètres des stratégies IPSec	
Encryption Algorithm	Choisissez l'algorithme de cryptage. Sélectionnez entre DES (8 caractères), 3DES (24 caractères), AES-128 (16 caractères) AES192 (24 caractères) et AES256 (32 caractères).
Integrity Algorithm	Choisissez un algorithme d'intégrité. Sélectionnez entre MD5 (16 caractères) et SHA-1 (20 caractères).
Paramètres de stratégie automatique (les 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'IPSec SA en secondes. La valeur par défaut est 7800 (130 minutes).
Paramètres de stratégie manuelle (les options s'affichent uniquement si la stratégie manuelle est sélectionnée)	
SPI Incoming	Entrez une valeur hexadécimale pour l'index des paramètres de sécurité entrants entre 0x100 et 0xffffffff.
SPI Outgoing	Entrez une valeur hexadécimale pour l'index des paramètres de sécurité sortants 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. Par exemple, la longueur de la clé pour 3DES compte 48 chiffres hexadécimaux.
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. Par exemple, MD5 compte 32 chiffres hexadécimaux et SHA-1 en compte 40.
Sélection du trafic local	
Local IP/IP Address/Subnet Mask	Déterminez les hôtes locaux qui seront autorisés à utiliser le VPN. Sélectionnez une adresse IP unique ou un sous-réseau (adresse IP et masque de sous-réseau).

Paramètres des stratégies IPSec	
Sélection du trafic à distance	
Remote IP/IP Address/Subnet Mask	Le trafic des hôtes locaux autorisés vers l'adresse IP ou le masque de sous-réseau à distance est routé via le tunnel VPN. Sélectionnez une adresse IP unique ou un sous-réseau (adresse IP et masque de sous-réseau).
Select IKE Policy	Choisissez une stratégie IKE à associer à cette stratégie IPSec. Pour afficher toutes les stratégies IKE, cliquez sur View IKE Table .

Page GRE Tunnel

Utilisez la page GRE Tunnel pour configurer la GRE (Generic Routing Encapsulation). GRE est un protocole de tunnellation développé par Cisco qui peut encapsuler une grande variété de types de paquets du protocole de couche réseau à l'intérieur des tunnels IP, créant ainsi une liaison point à point virtuelle au SRP à des points à distance sur un inter-réseau IP.

- ÉTAPE 1** Cliquez sur **VPN > GRE Tunnel** dans le panneau de navigation. La fenêtre *GRE Tunnel* s'ouvre.

À partir de cette page, vous pouvez afficher les tunnels GRE existants, modifier un tunnel GRE et ajouter un nouveau tunnel GRE. Vous pouvez également afficher les informations détaillées de chaque tunnel dans la liste des détails GRE.
- ÉTAPE 2** Pour ajouter un tunnel GRE, cliquez sur **Add Entry**. La fenêtre du nouveau tunnel GRE apparaît.
- ÉTAPE 3** Choisissez un nom d'identification pour le tunnel 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 dans les listes déroulantes. Si vous choisissez une valeur de clé, entrez sa valeur dans le champ Key Value. Vous pouvez entrer une valeur comprise entre 0 et 4294967295.
- ÉTAPE 6** Choisissez l'interface WAN via laquelle le tunnel doit être connecté. Par exemple : WAN1 ou WAN2. Le paramètre par défaut est System Default Route.
- ÉTAPE 7** Entrez l'adresse IP de destination du périphérique à distance qui terminera le nouveau tunnel.

ÉTAPE 8 Entrez l'adresse IP et le masque de sous-réseau de l'hôte à distance. Cliquez sur le bouton Add pour ajouter des adresses IP ou sur **Delete** pour supprimer une.

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

Paramètres de tunnel GRE	
Champ	Description
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 la 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	Sélectionnez 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 et 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 directions.
Key value	Si vous avez choisi une clé, entrez la valeur de la clé, comprise entre 0 et 4294967295.

Paramètres de tunnel GRE	
Champ	Description
WAN Interface Name	Choisissez l'interface WAN qui est utilisée pour créer le tunnel GRE avec l'hôte à distance.
Destination IP or HostName	Adresse IP ou FQDN du périphérique à distance qui terminera le tunnel.
Remote IP Address/Subnet Mask	Répertorie les hôtes à distance et les réseaux 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, puis cliquez sur Add . Pour supprimer une adresse, sélectionnez-la dans la liste des adresses IP à distance, puis cliquez sur Delete .

Page VPN Passthrough

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 SRP qui ont besoin de tunnels IPSec pour être installés indépendamment, tels que la connexion à un autre routeur sur le 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	
Champ	Description
IPSec Passthrough	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 Disabled .

Paramètres du transfert VPN	
Champ	Description
PPTP Passthrough	Le protocole de tunnellation point à point (PPTP) permet au protocole point à point d'être « tunnelisé » via un réseau IP. L'option PPTP PassThrough est activée par défaut. Pour désactiver le transfert PPTP, sélectionnez Disabled .
L2TP Passthrough	Le protocole L2TP (protocole de tunnellation couche 2) 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 désactiver le transfert L2TP, sélectionnez Disabled .

Page 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.
WINS2	Serveur WINS secondaire utilisé par les clients distants.

Paramètres du serveur Cisco VPN

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.

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 Management**
- **Page Time Setup**
- **Page User List**
- **Page User Privilege Control**
- **Page Log**
- **Page Factory Defaults**
- **Page Firmware Upgrade**
- **Page Backup & Restore**
- **Page Reboot**

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 correspondants et les règles d'accès à distance du SRP.

-
- ÉTAPE 1** Cliquez sur **Administration > Web Access Management**. La fenêtre *Web Access Management* s'ouvre.
- ÉTAPE 2** Configurez les paramètres d'accès à distance comme définis dans la table des paramètres de **Paramètres de la gestion de l'accès au Web**.
- ÉTAPE 3** Cliquez sur Submit pour enregistrer les paramètres.
-

Paramètres de la gestion de l'accès au Web	
Champ	Description
Accès au Web	
Web Utility Access	Sélectionnez HTTP et/ou HTTPS. Pour un accès à 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, où les x représente l'adresse IP de la passerelle sur Internet.
Web Utility Access via Wireless	Permet à l'administrateur d'accéder à l'utilitaire Web à partir d'un client sans fil local.
Accès distant	
Remote Management	Vous permet de gérer votre SRP à partir d'un emplacement distant via Internet.
Web Utility Access	Sélectionnez HTTP ou HTTPS. Pour un accès à 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 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 LAN.
Allowed Remote IP Address	Pour accéder au 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 le second bouton de radio 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 Management

Utilisez les pages de gestion à distance pour configurer les paramètres des éléments suivants :

- **TR069**
- **SNMP**
- **Local TFTP**

Pour accéder à ces pages, cliquez sur *Administration > Remote Management* de l'utilitaire de configuration.

TR069

Certains prestataires de services peuvent configurer automatiquement l'équipement de votre 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 **Administration > Remote Management > TR-069**. La fenêtre *TR-069* s'ouvre.

ÉTAPE 2 Cliquez sur **Enabled** pour permettre la configuration automatique du SRP à partir d'un serveur central. La valeur par défaut est Disabled.

ÉTAPE 3 Indiquez les paramètres TR-069 définis dans la table des **Paramètres TR-069**.

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

Paramètres TR-069	
Champ	Description
Status	Sélectionnez Enabled pour permettre la configuration automatique de votre routeur à partir d'un serveur central. La valeur par défaut est Disabled.

Paramètres TR-069	
Champ	Description
ACS URL	Entrez l'URL ACS fournie par votre prestataire de services. L'URL ACS est au format suivant : Protocole://hôte:port/chemin - Le protocole peut être http ou https. - L'hôte peut être un nom de domaine complet ou une adresse IP. - Le port est facultatif. - Le chemin est défini par l'ACS.
ACS Username	Le nom d'utilisateur pour l'ACS. Le nom d'utilisateur par défaut est le numéro de série OUI. Ce nom d'utilisateur doit correspondre à celui du serveur ACS.
ACS Password	The password for ACS. Ce mot de passe doit correspondre au nom d'utilisateur du serveur ACS.
Connection Request URL	Ce champ est automatiquement rempli. Le format est http://xxx.xxx.xxx.xxx:port. Les x représentent l'adresse IP du WAN du SRP.
Connection Request Username	Ce nom d'utilisateur doit correspondre à celui du serveur ACS.
Connection Request Password	Ce mot de passe doit correspondre au nom d'utilisateur du serveur ACS.
Periodic Inform Interval	Spécifiez l'intervalle (en secondes) auquel le SRP doit commencer les connexions à l'ACS. La valeur par défaut est de 86 400 secondes (24 heures).
Periodic Inform Enable	Sélectionnez Enabled pour permettre au routeur d'initier régulièrement des connexions à l'ACS. Sinon, sélectionnez Disabled .
Request Download	Cliquez sur Apply si vous souhaitez initier immédiatement une connexion à l'ACS. L'ACS appelle le RPC de téléchargement lorsqu'il reçoit la demande.

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. SNMP vous permet de surveiller et de contrôler les périphériques réseau, et de gérer les configurations, la collecte des statistiques, les performances et la sécurité. Le SRP prend en charge SNMPv2.

- ÉTAPE 1 Cliquez sur **Administration > Remote Management > SNMP**. La fenêtre *SNMP* s'ouvre.
- ÉTAPE 2 Pour activer le SNMP, cliquez sur **Enabled**.
- ÉTAPE 3 Sélectionnez un paramètre IP de confiance. Vous pouvez sélectionner **Any**, **Address** ou **Netmask**. Any n'est pas recommandé.
- ÉTAPE 4 Entrez les mots de passe de Get et Set Community.

Le mot de passe de Get Community permet d'obtenir un accès en lecture seule aux informations SNMP de la passerelle. Le mot de passe de Set Community permet d'obtenir un accès en lecture et en écriture.
- ÉTAPE 5 Cliquez sur Submit pour enregistrer les paramètres.

Paramètres SNMP	
Champ	Description
Enable/Disable	Pour activer l'identification de SNMP, cliquez sur Enabled. La valeur par défaut est Disabled.
Trusted IP	Sélectionnez Any pour permettre l'accès à partir de n'importe quelle adresse IP (non recommandé), ou entrez l'adresse IP et le masque de sous-réseau d'un seul gestionnaire ou de l'agent de déROUTement SNMP autorisé à accéder au SRP via SNMP.
Get Community	Entrez le mot de passe permettant d'accéder en lecture seule aux informations SNMP de la passerelle.
Set Community	Entrez le mot de passe permettant d'accéder en lecture/écriture aux informations SNMP de la passerelle.

Local TFTP

Utilisez la page du Local TFTP pour activer le SRP comme serveur TFTP. Lorsque vous activez le TFTP, vous pouvez télécharger des fichiers sur le SRP à distance, puis les utiliser en tant que serveur TFTP local pour servir des fichiers vers des hôtes sur le LAN tels que les téléphones IP.

- ÉTAPE 1** Cliquez sur **Administration > Remote Management > Local TFTP**. La fenêtre *Local TFTP Control* s'ouvre.
- ÉTAPE 2** Pour activer le TFTP, sélectionnez **Enabled**.
- ÉTAPE 3** Cliquez sur **Submit** pour enregistrer les paramètres.
- ÉTAPE 4** Entrez les paramètres de fichiers à distance définis dans la table des **Paramètres TFTP locaux**.

Paramètres TFTP locaux	
Champ	Description
TFTP	Sélectionnez Enabled pour activer le TFTP. Cette option est désactivée par défaut.
Obtenir les paramètres des fichiers à distance	
Interface	Interface utilisée pour obtenir le fichier à distance.
URL	Entrez l'URL de l'emplacement du fichier distant. Par exemple : http://www.votresite.com:port/chemin/nomdufichier ftp://nomdutilisateur:motdepasse@votresite:port/chemin/nomdufichier.
File	Entrez le nom du fichier distant.
Save As	Entrez le nom du fichier que vous enregistrez.
User Name	Entrez un nom d'utilisateur pour accéder au fichier distant
User Password	Entrez un mot de passe pour accéder au fichier distant.

Paramètres TFTP locaux	
Champ	Description
Timeout	Spécifiez la valeur d'expiration de la session (en secondes). Il s'agit de la durée maximale autorisée pour une session de connexion. L'expiration de la connexion pour les sessions HTTP et FTP est de 3 secondes. Celle des sessions TFTP est de 1 seconde. Pour les sessions HTTP et FTP, un message de réponse de réinitialisation TCP doit mettre fin à la session.
Retry	Spécifiez le nombre de nouvelles tentatives de sessions si un problème passager se produit au cours d'une session
Status	État du traitement du fichier distant.
File List table	Affiche le nom et la taille du fichier distant.

Page Time Setup

Utilisez la page Time Setup pour définir les paramètres du fuseau horaire de votre réseau. Vous pouvez configurer manuellement l'heure du système ou à l'aide du serveur NTP (Network Time Protocol).

- ÉTAPE 1** Cliquez sur **Administration > Time Setup**. La fenêtre *Time Setup* s'ouvre.
- ÉTAPE 2** Indiquez les paramètres de votre fuseau horaire. Le fuseau horaire est généralement appelé l'heure locale.
- ÉTAPE 3** Pour configurer manuellement l'horloge du système, sélectionnez **User Manual** et entrez la date et les fuseaux horaires. Entrez la date au format « année/mois/jour » et l'heure au format suivant : « heure : minutes : secondes »
- ÉTAPE 4** Pour régler automatiquement l'heure, configurez les paramètres des fuseaux horaires comme définis dans la table de **Paramètres de configuration de l'heure**.
- ÉTAPE 5** Cliquez sur **Submit** pour enregistrer les paramètres.

Paramètres de configuration de l'heure	
Champ	Description
User Manual	Pour configurer manuellement l'horloge du système, sélectionnez User Manual et entrez la date et les fuseaux horaires. Entrez la date au format « année/mois/jour » et l'heure au format suivant : « heure : minutes : secondes »
Fuseau horaire	
Regions	Entrez le fuseau horaire de votre région à partir de la liste déroulante. Par exemple : (GMT-8:00) Heure du Pacifique (USA & Canada).
Adjust Clock for Daylight Saving Changes	Sélectionnez cette option pour que le SRP règle automatiquement l'heure d'été.
Time Server Address	Pour utiliser le serveur NTP (Network Time Protocol) par défaut du SRP, sélectionnez Auto dans la liste déroulante. Il s'agit de la valeur par défaut. Si vous souhaitez spécifier le serveur NTP, sélectionner Manual , et entrez l'URL ou l'adresse IP du serveur NTP vous souhaitez utiliser.
Resync Timer	Entrez la valeur de l'intervalle du délai de resynchronisation (en secondes). Ce minuteur commande la fréquence des resynchronisations du SRP avec le serveur NTP. La valeur par défaut est 3 600 secondes.

Assistant de configuration

L'assistant de configuration vous guide à travers les principales étapes requises pour configurer votre SRP. Pour démarrer l'assistant de configuration, cliquez sur **Administration** sous l'onglet, puis cliquez sur **Setup Wizard** dans le volet de navigation. L'assistant de configuration s'affiche. Suivez les instructions de l'assistant de configuration de poursuivre l'installation.

Page User List

Utilisez la page User List pour gérer les utilisateurs qui ont accès à l'utilitaire de configuration.

Il existe deux comptes par défaut : **admin** et **cisco**. Le compte « admin » a un accès de niveau administrateur. Le compte « cisco » a un accès de niveau invité.

ÉTAPE 1 Cliquez sur **Administration > 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 Entrez un nouveau nom d'utilisateur.

REMARQUE Les noms d'utilisateur par défaut admin et cisco ne peuvent pas être modifiés.

ÉTAPE 4 Entrez l'ancien mot de passe (s'applique uniquement au compte Admin). Vous devez fournir votre ancien mot de passe lorsque vous modifiez le mot de passe.

ÉTAPE 5 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**.

REMARQUE Vous devez également fournir votre nouveau mot de passe lorsque vous accédez à l'utilitaire de configuration. Pour des raisons de sécurité, Cisco vous recommande vivement de modifier le mot de passe.

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

Page User Privilege Control

La page User Privilege Control permet à l'administrateur de régler les privilèges attribués à l'utilisateur.

ÉTAPE 1 Cliquez sur **Administration > User Privilege Control**. La fenêtre *User Privilege Control* s'ouvre.

ÉTAPE 2 Choisissez l'un des types d'accès pour chaque fonctionnalité.

- **Read/Write** : vous permet d'afficher et de configurer la page Web.
- **Read Only** : vous permet d'afficher la page Web.
- **Hidden** : masque le lien vers la page Web.

ÉTAPE 3 Cliquez sur **Apply** pour enregistrer votre paramètre.

Page Log

Le SRP vous permet d'enregistrer les listes entrantes, sortantes et de DHCP pour différents événements qui se produisent sur votre réseau. Le Incoming Log répertorie une liste temporaire des adresses IP et les numéros de port de destination de la source pour le trafic Internet entrant. Le Outgoing Log répertorie une liste temporaire des adresses IP, des URL/adresses IP de destination et le service/les numéros de port locaux pour le trafic Internet sortant.

ÉTAPE 1 Cliquez sur **Administration > Log**. La fenêtre *Log* s'ouvre.

ÉTAPE 2 Cliquez sur **Enabled** pour activer la consignation.

ÉTAPE 3 Sélectionnez le type de journal dans la zone de liste des journaux.

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

Paramètres de consignation

Champ	Description
Status	Pour accéder aux journaux de l'activité, sélectionnez Enabled. La consignation étant activée, vous pouvez afficher les fichiers journaux temporaires. Cliquez sur Disabled pour désactiver cette fonction.
Log List	Type de journal. Pour spécifier le type de journal, sélectionnez Incoming Log, Outgoing Log ou DHCP Client Log.

Page Factory Defaults

Utilisez la page Factory Defaults pour définir le SRP avec les paramètres avec lesquels il a été configuré lorsqu'il a été expédié de l'usine.

-
- ÉTAPE 1** Cliquez sur **Administration > Factory Defaults**. La fenêtre *Factory Defaults* s'ouvre.
 - ÉTAPE 2** Pour restaurer les paramètres d'usine du SRP, sélectionnez **Yes**. Tous les paramètres de données personnalisés (SRP) enregistrés précédemment seront perdus une fois les paramètres par défaut restaurés
 - ÉTAPE 3** Pour restaurer les paramètres de voix parmi les paramètres par défaut, sélectionnez **Yes**. Tous les paramètres de voix personnalisés sauvegardés précédemment seront perdus une fois les paramètres par défaut restaurés
 - ÉTAPE 4** Cliquez sur **Submit** pour enregistrer les paramètres.
-

Page Firmware Upgrade

Utilisez la page Firmware Upgrade pour mettre à niveau le microprogramme du SRP. 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 mettre à niveau le microprogramme, téléchargez le fichier de mise à niveau du microprogramme du SRP à l'adresse suivante : www.cisco.com/go/srp500 (en anglais). 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 **Browse** et sélectionnez l'emplacement du fichier de mise à niveau que vous avez téléchargé.
 - ÉTAPE 3** Cliquez sur le bouton **Upgrade**.
-



AVERTISSEMENT La mise à jour du microprogramme peut prendre quelques minutes. Tant le processus n'est pas terminé, NE mettez PAS l'alimentation hors tension, N'appuyez PAS sur le bouton de réinitialisation du matériel, ou NE cliquez PAS sur le bouton Précédent de votre navigateur actuel.

Page Backup & Restore

Cette section décrit comment sauvegarder et restaurer les paramètres de configuration du SRP. Il comprend les sections suivantes :

- **Page Backup Configuration**
- **Page Restore Configuration**

Pour accéder à ces pages, cliquez sur **Administration > Backup & Restore** dans l'utilitaire de configuration.

Page Backup Configuration

Utilisez la page Backup Configuration pour sauvegarder les paramètres de configuration du SRP dans un fichier. Vous pouvez désormais restaurer ultérieurement ces mêmes paramètres sur le 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 SRP.

Page Restore Configuration

Utilisez la page Restore Configuration pour restaurer les paramètres de configuration du SRP à partir d'une sauvegarde précédente. Vérifiez que vous avez sauvegardé les paramètres de configuration avant de restaurer la configuration.

-
- ÉTAPE 1** Cliquez sur **Administration > Backup & Restore > Restore Configuration**. La fenêtre *Restore Configuration* s'ouvre.
- ÉTAPE 2** Cliquez sur **Browse**, localisez le fichier de sauvegarde puis cliquez sur **Restore**.
-

Page Reboot

Utilisez la page Reboot pour mettre le SRP hors et sous tension (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 mettre le SRP hors et sous tension.
-

Page Status

Utilisez la page Status pour afficher l'état du CPU et de la mémoire du 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** : MIPS, charges et disponibilité.
- **Memory** : affiche l'espace totale de la mémoire (%), l'espace libre (%), l'espace utilisé (%), l'espace tampon (%), la taille du cache (%), l'espace actif et l'espace inactif (%)

Page Switch Setting

Sur les modèles DSL SRP526W et SRP527W, le port Ethernet 4 peut être configuré comme port WAN. Vous pouvez également définir la taille de paquet en mode « Jumbo » sur cet écran.

REMARQUE Lorsque le port Ethernet 4 est configuré comme port WAN, le port DSL devient inactif. Lorsque le port DSL est actif, le port Ethernet 4 fonctionne uniquement comme port LAN.

ÉTAPE 1 Cliquez sur **Administration > Switch Setting**.

La fenêtre *Switch Setting* s'ouvre.

ÉTAPE 2 Sélectionnez **Disable** pour configurer le port Ethernet 4 comme port WAN. Sélectionnez **Enable** pour activer le port DSL.

ÉTAPE 3 Choisissez une taille de paquet Jumbo.

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

Paramètres de commutation

Champ	Description
Interface DSL	Activez ou désactivez le port DSL. Une fois désactivé, le port LAN 4 peut être utilisé comme port WAN Ethernet.
Jumbo Mode	Taille du paquet Jumbo. Les options disponibles sont 1 522 ou 2 048 octets.

Utilisation des diagnostics de la plateforme prête pour les services

Ce chapitre décrit comment utiliser les fonctionnalités de diagnostic des plateformes prêtes pour les services.

- **Page Ping Test**
- **Page Traceroute Test**
- **Page Detect Active LAN Clients**

Pour accéder à ces pages, cliquez sur *l'onglet Diagnostics* dans la barre de menus 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 l'URL pour laquelle effectuer le test ping.
- 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 **Start to Ping** pour lancer le test. Une fois le test terminé, les résultats s'affichent sur la page.
- ÉTAPE 6** Cliquez sur **Close** pour fermer les résultats du test et afficher le formulaire.
-

Page Traceroute Test

Utilisez la page Traceroute Test 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** Saisissez l'adresse IP ou l'URL pour lancer le traçage.
 - ÉTAPE 3** Cliquez sur **Start to Traceroute** pour lancer le test. Les résultats s'affichent sur la page et sont actualisés toutes les 5 secondes.
 - ÉTAPE 4** Cliquez sur **Close** pour fermer les résultats et afficher le formulaire.
-

Page Detect Active LAN Clients

Utilisez la page Detect Active LAN Clients pour effectuer une recherche sur les clients actifs du LAN sur votre 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 **Start to Search** pour lancer le test. Une nouvelle fenêtre contenant les résultats du test s'affiche.
-

Affichage de l'état des plate-formes prêtes pour les services

Ce chapitre décrit comment afficher l'état de plates-formes prêtes pour les services.

- [Page Router](#)
- [Page Firewall Status](#)
- [Page Interface Information](#)
- [Page Wireless Network Status](#)
- [Page Wireless Client Information](#)
- [Page Mobile Network Status](#)
- [Page DHCP Server Information](#)
- [Page QoS Status](#)
- [Page Routing Table](#)
- [Page ARP Table](#)
- [Page RIP Status](#)
- [Page IGMP Status](#)
- [Page VPN Status](#)
- [Page CDP Neighbor Information](#)

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

Page Router

Utilisez la page Router pour afficher des informations sur le SRP et ses paramètres actuels.

Status > Router

Champ	Description
Model	Nom et fonctionnalités du produit.
Hardware Version	Numéro de version matérielle.
Boot Version	Numéro de version du microprogramme d'amorçage.
Firmware Version	Version actuelle du microprogramme.
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 définie sur le SRP.
WAN	Le type et le niveau de l'interface WAN.
LAN	L'interface LAN et le niveau.
Wireless	Nombre de SSID sans fil qui sont activés.

Page Firewall Status

Utilisez la page Firewall Status pour afficher les informations sur le pare-feu du SRP.

Status > Firewall

État du pare-feu	
Champ	Description
Stratégie d'accès à internet	
No	Numéro de la liste de stratégies d'accès à internet.
Policy Name	Identifiant numérique de la stratégie d'accès à internet.
Status	Affiche l'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)	Le volume du trafic passé par cette règle, en octets.
Blocked (pkts)	Nombre de paquets bloqués par cette règle.
Blocked (bytes)	Le volume du trafic bloqué par cette règle, en octets.
Port Forwarding	Affiche l'état des règles de transfert de port actuellement actives. Les règles qui ne sont pas activées ou qui sont associées aux 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 spécifié par l'utilisateur à transférer.
Host	Adresse IP de l'hôte LAN à transférer.
Packets	Nombre de paquets qui ont été transférés.
Traffic (bytes)	Volume du trafic qui a été transféré, en octets.
Statistics	Mesures générales du trafic via le pare-feu.

État du pare-feu	
Champ	Description
Name	Nom associé au traitement des paquets du pare-feu. ▪ INPUT : trafic destiné au SRP. ▪ OUTPUT : trafic provenant du SRP. ▪ FORWARD : trafic passé entre les réseaux public/externe et privé/interne.
Accept PKT	Nombre de paquets acceptés par ce chemin du pare-feu.
Accept Volume (bytes)	Le 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)	Le volume du trafic, en octets, filtré/bloqué par ce chemin du pare-feu.

Page Interface Information

Utilisez la page Interface Information pour afficher les informations relatives aux différentes interfaces.

Status > Interface

Informations sur l'interface	
Champ	Description
Liste des interfaces	
Interface	Répertorie les interfaces (IP) à trois couches LAN et WAN configurées. Une interface WAN Ethernet est affichée en tant que « WAN » et une interface WAN ADSL est affichée en tant que « PVC ». La numérotation des interfaces est dérivée comme suit : ▪ Interfaces principales : la numérotation suit l'étiquetage des ports physiques (c.-à-d. WAN1 et WAN2). ▪ Sous-interfaces WAN Ethernet : la numérotation reflète l'index VLAN configuré. ▪ PVC ADSL : numérotés en série de 0 à 3. ▪ VLAN Interfaces : 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.
Liste des ports	
Interface	Répertorie toutes les interfaces à deux couches (Ethernet, SSID WiFi, PVC DSL) LAN et WAN configurées.
TX (pkts)	Nombre de paquets transmis à partir de ce port.
RX (pkts)	Nombre de paquets reçus par ce port.

Informations sur l'interface	
Champ	Description
Status	État de connectivité du port.
Clear TX & RX	Cliquez sur ce bouton pour réinitialiser à 0 le nombre de paquets TX et RX.

Page Wireless Network Status

Utilisez la page Wireless Network Status pour afficher les informations relatives à vos réseaux sans fil.

Status > Wireless

État du réseau sans fil	
Champ	Description
Network Mode	Mode de fonctionnement configuré pour le point d'accès sans fil inclus. Pour plus d'informations, reportez-vous à la section Configuration du LAN sans fil , page 58.
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 Wireless Client Information pour afficher les informations sur les clients sans fil.

Status > Wireless Client Information

Informations sur le client sans fil	
Champ	Description
MAC Address	Adresse MAC du client.
Tx-Rate	Débit de données de transmission actuel du client.
Rx-Rate	Débit de données actuellement reçues par le 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 entrera en économie d'énergie si aucune activité ne se produit sur le lien.

Page Mobile Network Status

Utilisez la page Mobile Network Status pour afficher les informations pour le modem USB haut débit installé sur le SRP.

REMARQUE Cette page différera selon le type de modem USB que vous avez installé

Status > Mobile Network

Paramètres de la carte UMTS USB	
Champ	Description
IP Address	Adresse IP attribuée au modem USB.
Connection Up Time	Durée de la session de connexion actuelle.

Paramètres de la carte UMTS USB	
Champ	Description
Current Session Usage	Réception et transmission du volume du trafic.
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	Nombre d'IMSI de ce modem USB.
Service Type	Type de service de modem USB.
Signal Strength	Puissance du signal.
Card Status	L'état de la carte : En cours de connexion, Connectée, En cours de déconnexion, Déconnectée ou La carte n'est pas activée. Si aucune carte n'est jointe, la page d'état indique le message suivant concernant le SRP : « impossible de détecter le modem mobile USB ».

Paramètres de la carte USB CDMA2000 EVDO	
Champ	Description
IP Address	Adresse IP attribuée au modem USB.
Connection Up Time	Durée de la session de connexion actuelle.
Current Session Usage	Réception et transmission du volume du trafic.
Manufacturer	Fabricant du modem USB connecté.
Card Model	Nom de modèle du modem USB connecté.

Paramètres de la carte USB CDMA2000 EVDO	
Champ	Description
Card Firmware	Révision du microprogramme actuellement installée sur le modem USB.
ESN	Nombre d'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	L'état de la carte : En cours de connexion, Connectée, En cours de déconnexion, Déconnectée ou La carte n'est pas activée. Si aucune carte n'est jointe, la page d'état indique le message suivant concernant le SRP : « impossible de détecter le modem mobile USB ».

Page DHCP Server Information

Utilisez la page DHCP Server Information pour afficher les informations de location du serveur DHCP par règle.

Status > DHCP Server Information

DHCP Server Status	
Champ	Description
Client Name	Nom d'hôte du client DHCP.
IP Address	Adresse IP louée au client.
MAC Address	Adresse MAC du client DHCP.
Expires Time	Délai d'expiration de la location du DHCP actuelle.
Interface	Interface via laquelle le client est connecté.

Page QoS Status

Utilisez la page QoS Status pour afficher les statistiques de mise en file d'attente du trafic. Le SRP prend en charge 5 files d'attente : une file d'attente stricte et quatre files d'attente pondérées.

Status > QoS

État QoS	
Champ	Description
Queue Name	Répertorie les cinq files d'attente utilisées par le SRP.
Config Rate	La quantité nominale de trafic que chaque file d'attente peut prendre en charge dans les conditions équilibrées et chargés. Notez que la bande passante non utilisée par une file d'attente peut être utilisée par une autre, impliquant ainsi que la bande passante de mise en file d'attente configurée peut être dépassée.
Allow Maximum Rate	Le débit du trafic maximal, en Kbps, pour chaque file d'attente. Cela permet aux files d'attente pondérées d'utiliser toutes les bandes passante 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)	Le nombre d'octets envoyés à partir de cette file d'attente.
Send (pkts)	Le nombre de paquets envoyés à partir de cette file d'attente.
Drop	Nombre de paquets supprimés 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 à au débit maximal autorisé.
Requeues	Si un paquet ne peut pas être envoyé, il est remis dans la file d'attente d'origine permettant 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 Routing Table de routage pour afficher les informations sur le routage.

Status > Routing Table

État de la table de routage	
Champ	Description
Destination LAN IP	Adresse du réseau ou de l'hôte auquel la route statique est attribuée.
Subnet Mask	Indique quelle partie d'une adresse IP correspond à la partie réseau et quelle partie correspond à la partie hôte.
Gateway	L'adresse IP du périphérique passerelle qui permet le contact entre la passerelle 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).

Page ARP Table

Utilisez la page ARP Table pour afficher les informations sur toutes les entrées ARP (Protocole de résolution d'adresse).

Status > ARP Table

État de la table ARP	
Champ	Description
IP Address	Adresse IP du périphérique.
HW Type	Type de matériel du périphérique.
Flags	Type d'indicateur du périphérique.
HW Address	Adresse MAC du périphérique.

État de la table ARP	
Champ	Description
Mask	Masque du périphérique.
Device	Type d'interface du périphérique.

Page RIP Status

Utilisez la page RIP Status pour afficher les informations sur toutes les activités RIP (Protocole d'informations de routage). Pour accéder à cette page, cliquez sur **Status > RIP** dans l'utilitaire de configuration.

Cette page sauvegarde tous les messages RIP relatifs au daemon RIP associé. Pour chaque route reçue via RIP, elle affiche l'heure d'envoi du paquet et les informations sur les balises. Elle affiche également l'état RIP actuel, tel que le minuteur RIP, le filtrage, la version, l'interface activée par RIP et les informations sur les homologues RIP.

Page IGMP Status

Utilisez la page IGMP Status pour afficher les informations sur l'IGMP.

Status > IGMP

Champ	Description
IP Address	Adresse IP du périphérique.
Port	Port du périphérique.

Page VPN Status

Utilisez la page VPN Status pour afficher les informations sur l'état du VPN.

Status > VPN Status

État du VPN	
Champ	Description
Tunnel Name	Le nom du tunnel VPN.
Remote Policy	La stratégie de réseau à distance.
Local Policy	La stratégie réseau locale.
IKE Algorithm	Le résultat final de l'algorithme IKE après ISAKMP. S'applique uniquement au mode « AUTO ».
Upset Algorithm	L'algorithme IPSec que ce tunnel utilise actuellement.
TX Bytes	Le nombre d'octets transmis à partir de ce tunnel.
RX Bytes	Le nombre d'octets reçus de ce tunnel.
Connect Status	S'applique uniquement au mode « AUTO ».

Page CDP Neighbor Information

Utilisez la page CDP Neighbor Information pour afficher les informations sur le voisinage du CDP à partir de l'utilitaire de configuration.

REMARQUE Pour afficher des informations supplémentaires sur l'état, cliquez sur un élément de la liste Neighbor information. Le tableau CDP Details affiche des informations sur le périphérique sélectionné.

Status > CDP Neighbor Information

Informations sur le voisinage du CDP	
Champ	Description
Device ID	L'ID du périphérique du voisin.
Local Interface	Le nom du SRP local.
Hold Time	Le temps d'attente avant que le rejet de paquets par le CDP.
Capability	La classe du voisin.
Platform	Le système matériel du voisin.
Port ID	Le numéro de port du voisin.
IP Address	L'adresse IP du voisin.

Spécifications

Cette annexe répertorie les spécifications des modèles SRP520.

Fonctionnalité	SRP521W
WAN	Commutateurs
LAN	4 ports Fast Ethernet
Sans fil	802.11b/g/n
Température de fonctionnement	0 °C à 40 °C
Température de stockage	-20 °C à 70 °C
Humidité de fonctionnement	De 10 à 85 %, sans condensation
Humidité de stockage	De 5 à 90 %, sans condensation
Plage de tension	100-240 V 50/60 Hz CA
Dimensions	(L x P x H) : 170 mm x 170 mm x 42 mm
Poids	400 g

Fonctionnalité	SRP526W
WAN	ADSL2+ Annexe B
LAN	4 ports Fast Ethernet
Sans fil	802.11b/g/n
Température de fonctionnement	0 °C à 40 °C

Fonctionnalité	SRP526W
Température de stockage	-20 °C à 70 °C
Humidité de fonctionnement	De 10 à 85 %, sans condensation
Humidité de stockage	De 5 à 90 %, sans condensation
Plage de tension	100-240V 50/60 Hz CA
Dimensions	(L x P x H) : 170 mm x 170 mm x 42 mm
Poids	440 g

Fonctionnalité	SRP 527W
WAN	ADSL2+ Annexe A
LAN	4 ports Fast Ethernet
Sans fil	802.11b/g/n
Température de fonctionnement	0 °C à 40 °C
Température de stockage	-20 °C à 70 °C
Humidité de fonctionnement	De 10 à 85 %, sans condensation
Humidité de stockage	De 5 à 90 %, sans condensation
Plage de tension	100-240V 50/60 Hz CA
Dimensions	(L x P x H) : 170 mm x 170 mm x 42 mm
Poids	440 g

Pour en savoir plus

Cisco propose une vaste gamme de ressources pour vous aider, ainsi que votre client, 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