GUIDE D'ADMINISTRATION

CiscoSmallBusiness
GammeRV0xx Routeurs

RV042 - Routeur VPN double WAN
RV042G - Routeur VPN double WAN Gigabit
RV082 - Routeur VPN double WAN
RV016 - Routeur VPN multi-WAN

78-19649-01B0

Table des matières

1

Introduction

Nous vous remercions d'avoir choisi le Routeurs VPN de la gamme CiscoRV0xx. Ce guide fournit des informations détaillées sur la configuration et la gestion de votre routeur. Ce chapitre comprend des informations qui vous seront utiles pour commencer à utiliser votre routeur. Reportez-vous aux rubriques suivantes:

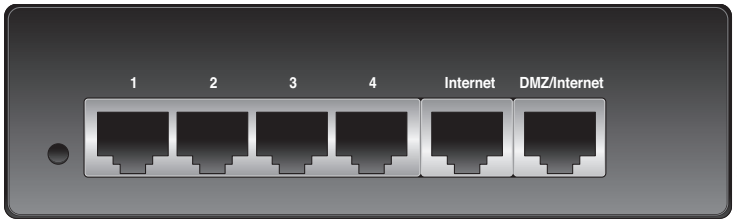
Caractéristiques des routeurs de la gamme RV0xx

Les routeurs Cisco de la gamme RV0xx double WAN et les routeurs VPN multi-WAN offrent des solutions de connectivité fiables, hautement sécurisées et hautes performances. Tous ces routeurs prennent en charge une seconde connexion à Internet. Cela permet d'obtenir une connectivité continue et de disposer d'une bande passante disponible plus large. En outre, cette seconde connexion contribue à l'équilibrage du trafic. Il existe trois modèles, dont vous trouverez une comparaison dans le tableau ci-après.

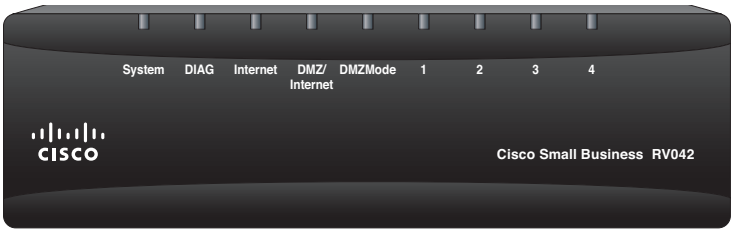
Modèle	Ports LAN	Ports WAN/DMZ
RV042 et RV042G	4	2
RV082	8	2
RV016	8 à 13	2 à 7 Internet 1 DMZ

REMARQUE Les modèles RV042, RV042G et RV082 sont dotés d'un port Internet dédié et d'un port mixte DMZ/Internet. Le modèle RV016 est doté de deux ports Internet dédiés, d'un port DMZ dédié (demilitarized zone, zone démilitarisée) et de cinq ports mixtes pouvant être configurés en tant que ports LAN (local area network, réseau local) ou en tant que ports Internet.

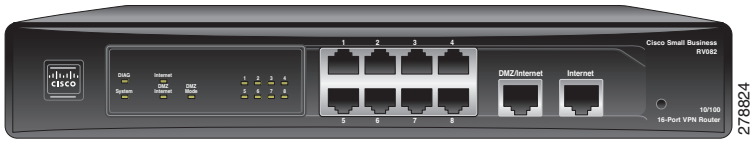
Ports RV042 et RV042G



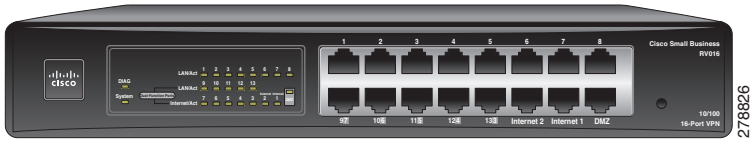
Voyants d'état RV042 et RV042G



Ports RV082 et voyants d'état



Ports RV016 et voyants d'état



Ports

Port	Description
Internet (RV042 et RV082) ou Internet 1-2 (RV016)	Utilisez ce port pour relier le routeur à un service réseau à large bande.
DMZ/Internet (RV042 et RV082)	Utilisez ce port pour connecter le routeur à un second périphérique réseau haut débit ou à un hôte DMZ tel qu'un serveur Web ou un serveur FTP. Les connexions DMZ permettent au trafic Internet public d'accéder à un ordinateur spécifique de votre réseau sans mettre en danger votre réseau LAN.
DMZ (RV016)	Utilisez ce port pour connecter le routeur à un hôte DMZ tel qu'un serveur Web ou un serveur FTP. Les connexions DMZ permettent au trafic Internet public d'accéder à un ordinateur spécifique de votre réseau sans mettre en danger votre réseau LAN.
1 à 4 (RV042 et RV042G) ou 1 à 8 (RV082 et RV016)	Utilisez ces ports numérotés pour connecter des ordinateurs et d'autres périphériques du réseau local.
Ports mixtes 9 à 13 et 3 à 7 (RV016)	Utilisez ces ports en tant que ports LAN (ports numérotés de 9 à 13) ou configurez-les en tant que ports Internet (ports numérotés de 3 à 7). Leur état est indiqué par les voyants d'état correspondants: LAN/Act 9 à 13 ou Internet/Act 3 à 7.

Voyants d'état

Voyant	Description
DIAG	**Allumé:** le routeur est en cours de préparation à l'utilisation. **Éteint:** le routeur est prêt à être utilisé.
Système	**Fixe:** le routeur est allumé. **Clignotant:** le routeur effectue un test de diagnostic.
Internet (RV082, RV042 et RV042G) ou Internet 1-2 (RV016)	**Fixe:** un périphérique est connecté au port Internet. **Clignotant:** activité réseau au niveau du port Internet.
DMZ/Internet (RV082, RV042, RV042G) ou DMZ (RV016)	**Fixe:** un périphérique est connecté au port DMZ/Internet ou au port DMZ. **Clignotant:** activité réseau au niveau du port.
Mode DMZ (RV082, RV042, RV042G)	**Allumé:** le port DMZ/Internet est configuré comme port DMZ. **Éteint:** le port DMZ/Internet est configuré comme connexion Internet secondaire.
1 à 4, 1 à 8	**Fixe:** un périphérique est connecté au port LAN numéroté. **Clignotant:** activité réseau au niveau du port numéroté.
Ports RV042G Gigabit	Pour les ports Internet, DMZ/Internet et numérotés, la couleur de la barre indique le débit. **Vert:** Gigabit. **Orange:** 10/100M.
Ports mixtes RV016 :	
LAN/Act 9 à 13	Allumé si le port est configuré comme port LAN. **Fixe:** un périphérique est connecté au port. **Clignotant:** activité réseau au niveau du port.

Voyant	Description
Internet/Act 3 à 7 (RV016)	Allumé si le port est configuré comme port Internet. **Fixe:** un périphérique est connecté au port. **Clignotant:** activité réseau au niveau du port.

Autres caractéristiques matérielles

Fonctionnalité	Description
Réinitialiser	Le bouton de réinitialisation est un bouton noir en retrait. Vous trouverez ce bouton près du port n°1 sur le panneau arrière des modèles RV042 et RV042G et à proximité des ports Internet et DMZ sur le panneau avant des modèles RV082 et RV016. ▪ **Pour redémarrer le routeur ou restaurer la connexion:** si le routeur rencontre des difficultés pour se connecter à Internet, appuyez sur le bouton Reset, avec la pointe d'un stylo et maintenez-le enfoncé pendant une seconde. ▪ **Pour restaurer les paramètres d'usine par défaut:** si le routeur rencontre des problèmes graves et que vous avez épuisé en vain toutes les autres méthodes de dépannage, appuyez sur le bouton Reset et maintenez-le enfoncé pendant 30secondes pour restaurer les paramètres d'usine par défaut. Tous les paramètres antérieurs seront effacés.
Logement de sécurité	Utilisez le logement de sécurité situé sur le panneau latéral du routeur pour fixer un verrou de protection contre le vol.

Fonctionnalité	Description
Alimentation	▪ **RV042 et RV042G:** branchez l'adaptateur secteur fourni sur le port d'alimentation situé sur le panneau latéral du routeur. ▪ **RV082 et RV016:** branchez le câble d'alimentation CA fourni sur le port d'alimentation situé sur le panneau arrière du routeur.

Paramètres par défaut

Paramètre	Valeur par défaut
Nom d'utilisateur	admin
Mot de passe	admin
Adresse IP LAN	192.168.1.1
Plage DHCP	192.168.1.100 à 149
Masque réseau	255.255.255.0

Options de montage

Choix de l'emplacement

- **Température ambiante:** pour éviter tout risque de surchauffe du routeur, ne l'utilisez pas dans les lieux où la température ambiante dépasse 40°C.
- **Circulation de l'air:** assurez-vous que la circulation de l'air est suffisante autour du routeur.
- **Charge mécanique:** assurez-vous que le routeur est à niveau et stable, afin d'éviter tout danger.

Installation sur un bureau

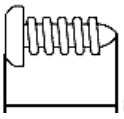
Avant d'installer le routeur sur un bureau, collez les quatre pastilles adhésives sur le panneau inférieur. Placez le routeur sur une surface plane, à proximité d'une prise électrique.

AVERTISSEMENT Ne posez aucun objet sur le routeur: toute charge excessive risquerait de l'endommager.

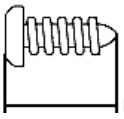
Montage mural

Le panneau inférieur du routeur comporte deux orifices de montage mural. Pour monter le routeur contre un mur, vous aurez besoin de matériel supplémentaire (non fourni). Nous vous suggérons d'utiliser le matériel illustré ci-après (l'échelle n'est pas respectée).

Suggestion de matériel pour les modèles RV042 et RV042G

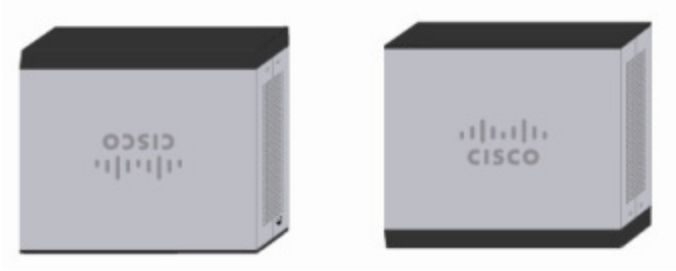
	
5 à 5,5mm	20 à 22mm

Suggestion de matériel pour les modèles RV082 et RV016

	
6,5 à 7mm	16,5 à 18,5mm

AVERTISSEMENT Le montage incorrect de l'appareil peut provoquer des dommages matériels et des blessures corporelles. Cisco n'est pas responsable des dommages causés par le montage mural incorrect de l'appareil.

AVERTISSEMENT Pour votre sécurité, assurez-vous que les orifices de dissipation thermique sont orientés vers le côté..



STEP 1 Percez deux trous d'implémentation dans la surface d'installation.

- **RV042 et RV042G:** écart de 58mm
- **RV082 et RV016:** écart de 94mm

STEP 2 Insérez une vis dans chaque trou en conservant un espace de 1 à 1,2mm entre la surface et la base des têtes de vis.

STEP 3 Placez les orifices de fixation murale du routeur sur les vis et faites glisser le routeur vers le bas jusqu'à ce que les vis se logent parfaitement dans les orifices.

Montage sur bâti des modèles RV082 et RV016

Vous pouvez monter les modèles RV082 et RV016 dans un bâti de taille standard d'environ 48cm (19pouces) de largeur. Le routeur nécessite un espace de 1RU (rack unit, unité de bâti), ce qui correspond à une hauteur de 44,45mm (1,75pouce). Les supports de montage sont fournis.

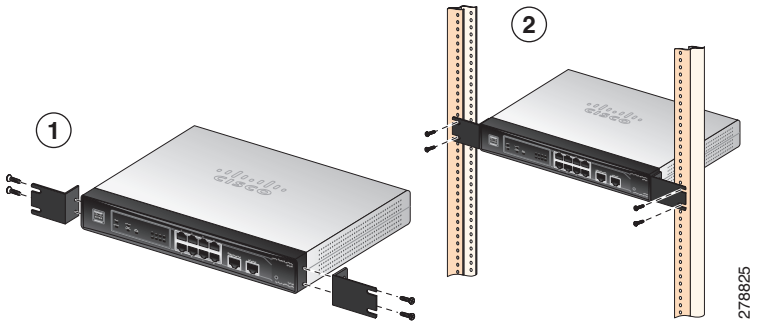
ATTENTION Lorsque vous installez plusieurs appareils dans un bâti, évitez de surcharger la prise ou le circuit électrique.

STEP 1 Placez le routeur sur une surface plane et dure.

STEP 2 Fixez un des supports de montage sur bâti fournis sur un côté du routeur, à l'aide des vis fournies. Serrez fermement les vis du support.

STEP 3 Procédez de la même manière pour fixer le second support sur le côté opposé.

STEP 4 Utilisez des vis appropriées pour fixer correctement les supports au bâti de 19pouces.



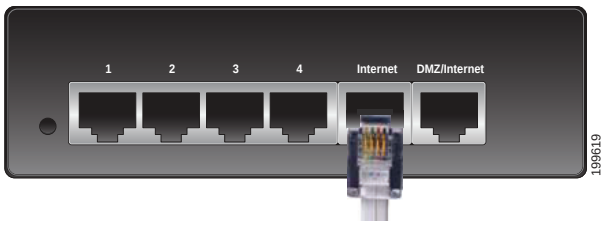
Connexion du matériel

STEP 1 Assurez-vous que tous les périphériques réseau sont hors tension, notamment le routeur, les ordinateurs, les commutateurs Ethernet et le périphérique réseau haut débit (modem DSL ou câble).

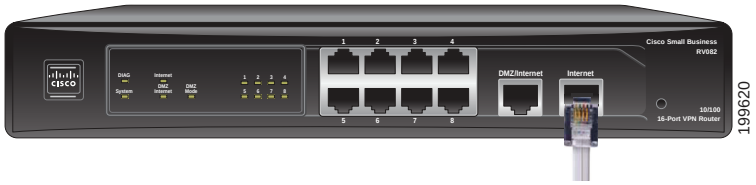
STEP 2 Pour vous connecter au service Internet:

- **RV042, RV042G et RV082:** reliez le périphérique réseau haut débit au port **Internet** du routeur à l'aide d'un câble Ethernet.

  Ports Internet RV042 et RV042G

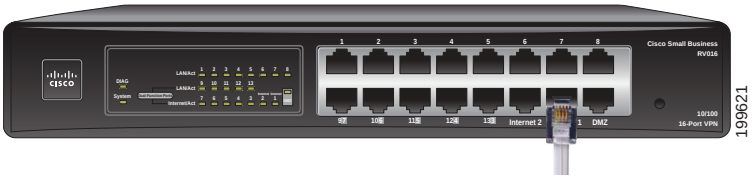


Port Internet du modèleRV082



- **RV016:** reliez le périphérique réseau haut débit au port **Internet 1** du routeur à l'aide d'un câble Ethernet.

Port Internet1 du modèleRV016



STEP 3 Pour vous connecter à un service Internet secondaire:

- **RV042, RV042G et RV082:** reliez le port **DMZ/Internet** au second périphérique réseau à large bande à l'aide d'un câble Ethernet.
- **RV016:** reliez le port **Internet2** au second périphérique réseau à large bande à l'aide d'un câble Ethernet.

STEP 4 Pour connecter un ordinateur ou un serveur qui servira d'hôte DMZ:

- **RV042, RV042G et RV082:** reliez le port **DMZ/Internet** à l'hôte DMZ à l'aide d'un câble Ethernet.
- **RV016:** reliez le port **DMZ** à l'hôte DMZ à l'aide d'un câble Ethernet.

STEP 5 Pour connecter d'autres périphériques réseau, tels que des ordinateurs, des serveurs d'impression et des commutateurs Ethernet, reliez un port LAN numéroté au périphérique réseau, à l'aide d'un câble Ethernet.

STEP 6 Mettez le ou les périphériques réseau à large bande sous tension.

STEP 7 Branchez le routeur sur une prise électrique, à l'aide d'un adaptateur secteur (RV042 et RV042G) ou d'un câble d'alimentation (RV082 et RV016). Le voyant d'état Système est vert.

STEP 8 Mettez les autres périphériques réseau sous tension.

Mise en route du programme de configuration

STEP 1 Connectez un ordinateur à un port LAN numéroté du routeur. Votre ordinateur devient un client DHCP du routeur et reçoit une adresse IP comprise dans la plage 192.168.1.x.

STEP 2 Ouvrez un navigateur Web. Pour pouvoir utiliser l'utilitaire de configuration, vous devez disposer d'un ordinateur sur lequel est installé Internet Explorer (version6 ou supérieure), Firefox ou Safari (pour Mac).

STEP 3 Dans la barre d'adresse, saisissez l'adresseIP par défaut du routeur, à savoir **192.168.1.1**

STEP 4 Lorsque la page de connexion s'affiche, saisissez le nom d'utilisateur par défaut **(admin)** et le mot de passe par défaut **(admin),** en lettres minuscules.

STEP 5 Cliquez sur **Login**. La page *System Summary* s'affiche.

Les paramètres par défaut du routeur sont suffisants pour la plupart des petites entreprises. Toutefois, votre fournisseur d'accès à Internet vous demandera peut-être de configurer des paramètres supplémentaires. Sur la page *System Summary*, vérifiez l'état du WAN pour savoir si le routeur a obtenu une adresse IP. Dans la négative, passez à l'étape suivante.

STEP 6 Pour configurer votre connexion Internet à l'aide de l'Assistant de configuration, cliquez sur **Setup Wizard** sur la page *System Summary* ou cliquez sur **Wizard,** dans l'arborescence. Dans la section *Basic Setup* , cliquez sur **Launch Now**. Suivez les instructions affichées à l'écran.

Si votre navigateur Web affiche un message d'alerte relatif à la fenêtre contextuelle, autorisez le contenu bloqué.

STEP 7 Pour configurer d'autres paramètres, cliquez sur les liens de l'arborescence.

Cisco vous recommande vivement de définir un mot de passe d'administrateur sécurisé, afin d'éviter tout accès non autorisé à votre routeur.

Conseils de dépannage

Si vous ne parvenez pas à vous connecter à Internet ni à l'utilitaire Web de configuration:

- Vérifiez que votre navigateur Web n'est pas configuré pour travailler hors connexion.
- Vérifiez les paramètres de la connexion locale de votre adaptateur Ethernet. L'ordinateur doit obtenir une adresse IP via le protocole DHCP. Il peut également disposer d'une adresse IP statique comprise dans la plage 192.168.1.x, lorsque la passerelle par défaut est définie sur 192.168.1.1 (adresseIP par défaut du routeur).
- Vérifiez que les paramètres que vous avez saisis dans l'Assistant pour configurer votre connexion Internet sont corrects, notamment le nom d'utilisateur et le mot de passe, le cas échéant.
- Essayez de réinitialiser le modem et le routeur, en mettant ces deux appareils hors tension. Ensuite, mettez le modem sous tension et patientez pendant 2minutes environ. Mettez le routeur sous tension. Vous devriez alors recevoir une adresse IP WAN.
- Vérifiez la plage d'adresses IP DHCP de votre modem. Si le modem utilise la plage 192.168.1.x, déconnectez le câble reliant le modem au routeur, puis démarrez l'utilitaire de configuration du routeur. Dans l'arborescence, cliquez sur **Setup > Network**. Saisissez une nouvelle adresse IP pour le périphérique, par exemple 10.1.1.1 ou 192.168.0.1. Si votre modem est de type DSL, vous pouvez également laisser tous les paramètres inchangés et demander à votre fournisseur d'accès à Internet de basculer le modem DSL en mode pont.

Caractéristiques de l'interface utilisateur

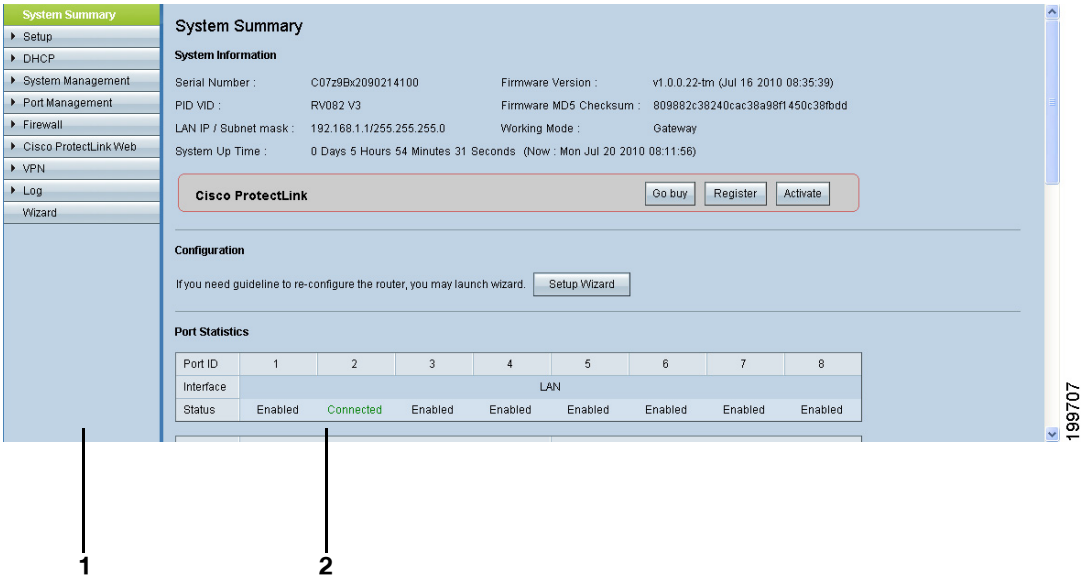
L'interface utilisateur est conçue pour faciliter la configuration et la gestion de votre routeur. Reportez-vous aux rubriques suivantes:

- **Navigation, page 19**
- **Fenêtres contextuelles, page 19**
- **Assistants de configuration, page 20**
- **Enregistrement des paramètres, page 20**

- **Aide, page 20**
- **Déconnexion, page 20**

Navigation

Les modules principaux de l'utilitaire de configuration sont représentés par des boutons, dans le volet de navigation gauche. Cliquez sur un bouton, pour afficher d'autres options. Cliquez sur une option, pour ouvrir une page de configuration. La page sélectionnée s'affiche dans la fenêtre principale de l'utilitaire de configuration.



1. Arborescence de navigation
2. Page de configuration

Fenêtres contextuelles

Certains liens et boutons déclenchent l'apparition de fenêtres contextuelles contenant des informations supplémentaires ou les pages de configuration associées. Si votre navigateur Web affiche un message d'alerte relatif à la fenêtre contextuelle, autorisez le contenu bloqué.

Assistants de configuration

Deux assistants de configuration aident à configurer votre connexion Internet et/ou votre configuration DMZ et les règles d'accès relatives aux réseaux WAN, LAN et DMZ. Vous pouvez utiliser ces assistants ou les autres pages de l'utilitaire de configuration.

Pour ouvrir la page de l'assistant: cliquez sur le bouton **Setup Wizard** dans la page *System Summary*, section *Configuration*. Vous pouvez également cliquer sur **Wizard**, dans l'arborescence de navigation. Deux assistants sont disponibles:

- **Basic Setup:** cliquez sur **Launch Now** pour configurer les paramètres de base de DMZ et de votre connexion Internet. Suivez les instructions affichées à l'écran.
- **Access Rule Setup:** cliquez sur **Launch Now** pour configurer des règles d'accès pour les réseaux WAN, LAN et DMZ. Suivez les instructions affichées à l'écran.

Enregistrement des paramètres

Les paramètres que vous avez définis sur la page de configuration ne sont pas enregistrés tant que vous n'avez pas cliqué sur le bouton **Save**. Lorsque vous naviguez vers une autre page, tout paramètre non enregistré est abandonné.

Pour effacer les paramètres sans les enregistrer, cliquez sur le bouton **Cancel**.

Aide

Pour afficher des informations supplémentaires sur la page de configuration sélectionnée, cliquez sur le lien **Help** situé près du coin supérieur droit de l'utilitaire de configuration. Si votre navigateur Web affiche un message d'alerte relatif à la fenêtre contextuelle, autorisez le contenu bloqué.

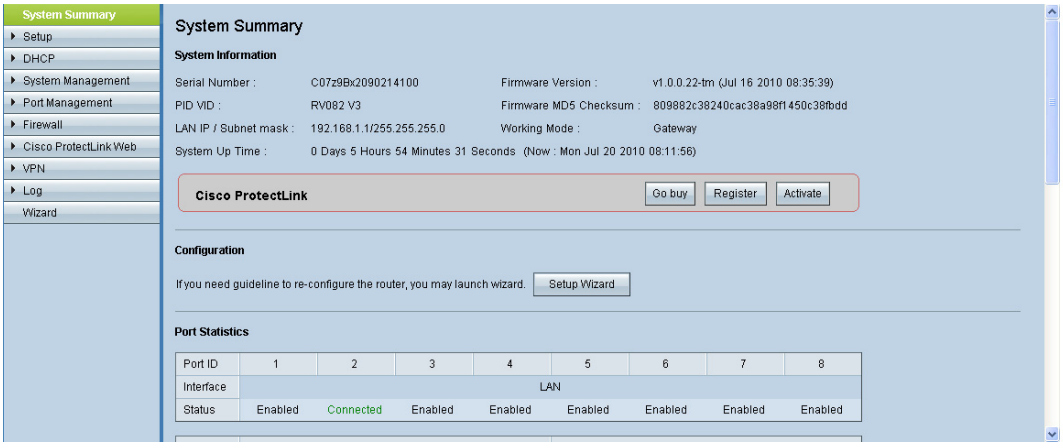
Déconnexion

Pour quitter l'utilitaire de configuration, cliquez sur le lien **Logout** situé près du coin supérieur droit de l'utilitaire de configuration. La page de connexion *Login* apparaît. Vous pouvez fermer la fenêtre du navigateur.

2

Affichage du résumé des informations système

La page *System Summary* apparaît une fois que vous êtes connecté à l'utilitaire de configuration. Vous pouvez également afficher cette page en cliquant sur **System Summary** dans l'arborescence de navigation. Utilisez cette page pour afficher les informations relatives à l'état actuel du routeur et des paramètres. Reportez-vous aux rubriques suivantes:



System Information

Cette section contient les informations suivantes:

- **Serial Number:** numéro de série du routeur.
- **Firmware version:** numéro de la version actuelle du microprogramme installée sur le routeur.
- **PID VID:** numéro de la version actuelle du matériel.
- **MD5 Checksum:** valeur utilisée pour la validation de fichiers.
- **LAN IP / Subnet mask:** adresseIP actuelle du routeur sur le réseau local.
- **Working Mode:** mode de fonctionnement (passerelle ou routeur).
- **LAN:** si l'adresse IP Dual-Stack est activée dans la page *Setup* > *Network*, cette section affiche l'adresseIPv4 et le masque de sous-réseau ainsi que l'adresse IPv6 et la longueur de préfixe.
- **System Up time:** durée en jours, heures et minutes d'activité du routeur.

Cisco ProtectLink Web

Cette section affiche des boutons correspondant au service Cisco ProtectLink Web facultatif. ProtectLink Web permet de sécuriser votre réseau. Il filtre les adresses de site Web (URL) et bloque les sites Web potentiellement malveillants. (Reportez-vous également au **Chapitre 8, « Mise en route de CiscoProtectLink Web ».**)

REMARQUE Ce service n'est pas disponible sur Cisco RV042G.

Vous pouvez utiliser les boutons suivants:

- **Go buy:** cliquez sur ce bouton pour acheter une licence d'utilisation. Vous serez dirigé vers la liste des revendeurs Cisco, sur le site Web Cisco. Suivez ensuite les instructions affichées à l'écran.
- **Register:** cliquez sur ce bouton si vous disposez d'une licence mais que vous ne l'avez pas encore enregistrée. Vous serez dirigé vers sur le site Cisco ProtectLink Web. Suivez ensuite les instructions affichées à l'écran.
- **Activate:** cliquez sur ce bouton si vous avez enregistré le service Cisco ProtectLink Web et que vous souhaitez l'activer. Vous serez dirigé vers sur le site Cisco ProtectLink Web. Suivez les instructions affichées à l'écran.

REMARQUE Si les options Cisco ProtectLink Web ne sont pas affichées dans la page *System Summary*, vous pouvez mettre à niveau le microprogramme du routeur pour activer cette fonctionnalité.

Configuration

Si vous avez besoin d'aide pour configurer le routeur, cliquez sur **Setup Wizard**. Vous pouvez alors utiliser les assistants suivants:

- **Basic Setup Wizard:** utilisez cet assistant pour configurer votre connexion Internet.
- **Access Rule Setup Wizard:** utilisez cet assistant pour configurer la stratégie de sécurité de votre VPN.

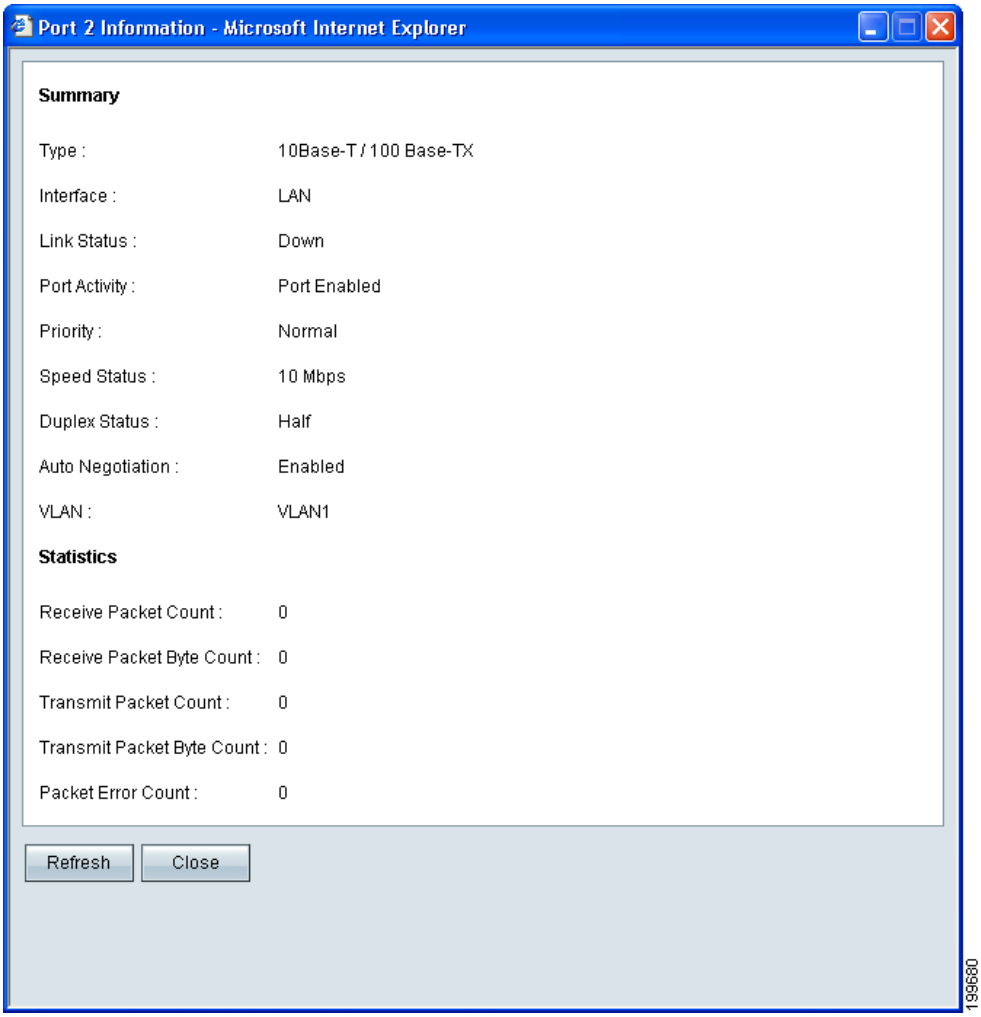
Port Statistics

Ce tableau indique l'état et les statistiques disponibles de chaque port. Il permet également d'accéder à des informations détaillées sur l'activité actuelle d'une liaison.

- **Port ID:** libellé du port.
- **Interface:** type d'interface, par exemple LAN, WAN ou DMZ. Les différentes interfaces WAN sont identifiées par un numéro, par exemple WAN1 et WAN2.
- **Status:** état du port: *Disabled* (rouge), *Enabled* (noir) ou *Connected* (vert). L'état est un lien hypertexte sur lequel vous pouvez cliquer pour ouvrir la fenêtre *Port Information*.

  Fenêtre Port Information

  Si vous cliquez sur un état dans le tableau *Port Statistics*, la fenêtre *Port Information* s'affiche. Cette fenêtre contient les informations les plus récentes relatives à l'interface et à l'activité actuelle. Pour mettre à jour les informations affichées, cliquez sur le bouton **Refresh**. Pour fermer la fenêtre, cliquez sur le bouton **Close**.



Cette fenêtre contient les informations suivantes:

- **Type:** type de port, par exemple 10Base-T/100 Base-TX.
- **Interface:** type d'interface, par exemple LAN, DMZ ou WAN.
- **Link Status:** état actuel de la liaison (*Up* ou *Down*).
- **Port Activity:** activité actuelle sur le port: Port Enabled, Port Disabled ou Port Connected.
- **Priority:** paramètre de priorité: High ou Normal.
- **Speed Status:** vitesse; 10Mbits/s ou 100Mbits/s.
- **Duplex Status:** mode duplex; Half ou Full.

- **Auto negotiation:** paramètre de négociation automatique; On ou Off.
- **VLAN:** ID du VLAN.
- **Receive Packet Count:** nombre de paquets reçus par le biais de ce port.
- **Receive Packet Byte Count:** nombre d'octets reçus par le biais de ce port.
- **Transmit Packet Count:** nombre de paquets transmis par le biais de ce port.
- **Transmit Packet Byte Count:** nombre d'octets transmis par le biais de ce port.
- **Packet Error Count:** nombre d'erreurs de paquets.

WAN Status

Cette section affiche des informations concernant l'interface WAN1 et l'interface DMZ ou WAN2, selon votre configuration. Sur le routeur Cisco RV016, d'autres interfaces WAN peuvent être configurées. Utilisez les onglets pour afficher les informations IPv4 et IPv6.

REMARQUE L'onglet IPv6 n'est disponible que si vous avez activé l'adresse IP Dual-Stack dans la page *Setup> Network*.

- **Informations de WAN:**
  - **IP Address:** adresse IP publique actuelle de cette interface.
  - **Default Gateway:** passerelle par défaut pour cette interface.
  - **DNS:** adresseIP du serveur DNS pour cette interface.
  - **Dynamic DNS (IPv4 uniquement):** paramètres DDNS pour ce port (Disabled ou Enabled).
  - **Release** et **Renew**: ces boutons apparaissent si le port est défini de façon à obtenir une adresseIP automatiquement. Cliquez sur **Release** pour libérer l'adresseIP, puis cliquez sur **Renew** pour mettre à jour la durée du bail DHCP ou pour obtenir une nouvelle adresseIP.
  - **Connect** et **Disconnect**: ces boutons apparaissent si le port est défini sur PPPoE ou PPTP. Cliquez sur **Disconnect** pour vous déconnecter du service Internet. Cliquez sur **Connect** pour rétablir la connexion.

- **Informations de DMZ:**
  - **IP Address:** adresse IP publique actuelle de cette interface.
  - **DMZ Host:** adresse IP privée de DMZ de l'hôte DMZ. La valeur par défaut est **Disabled**.

Firewall Setting Status

Cette section contient les informations suivantes:

- **SPI (Stateful Packet Inspection):** état de la fonctionnalité de négociation automatique: *On* (vert) ou *Off* (rouge).
- **DoS (Denial of Service) :** état de cette fonctionnalité, *On* (vert) ou *Off* (rouge).
- **Block WAN Requests:** état de cette fonctionnalité, *On* (vert) ou *Off* (rouge).
- **Gestion à distance :** état de cette fonctionnalité, *On* (vert) ou *Off* (rouge).
- **Access Rule:** nombre de règles d'accès définies.

VPN Setting Status

Cette section contient les informations suivantes:

- **Tunnel(s) Used:** nombre de tunnels VPN utilisés.
- **Tunnel(s) Available:** nombre de tunnels VPN disponibles.

Log Setting Status

Cette section contient les informations suivantes:

- **Syslog Server:** état du serveur syslog, *On* (vert) ou *Off* (rouge).
- **Email Log :** état du journal de messagerie, *On* (vert) ou *Off* (rouge).

3

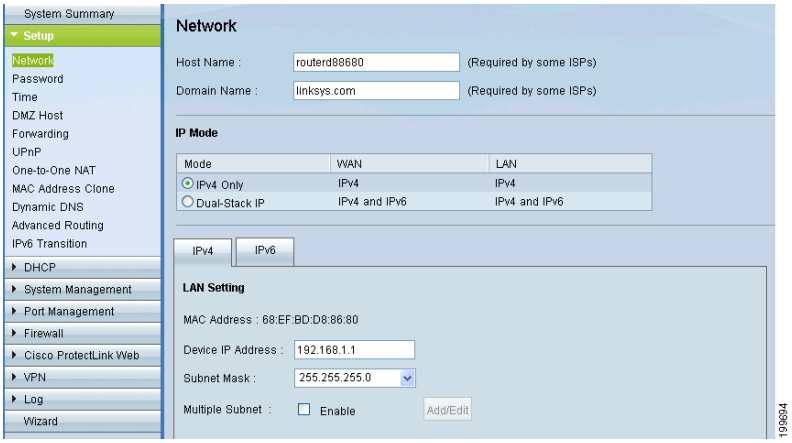
Configuration

Utilisez le module *Setup* pour configurer les fonctions de base du routeur. Reportez-vous aux rubriques suivantes:

Configuration du réseau

Utilisez la page *Setup > Network* pour configurer votre réseau LAN, votre réseau WAN (connexions Internet) et l'interface DMZ.

Pour ouvrir cette page: cliquez sur **Setup> Network** dans l'arborescence.



REMARQUE Avant de quitter cette page, cliquez sur **Save** pour enregistrer vos paramètres ou sur **Cancel** pour les annuler. Les modifications non enregistrées ne sont pas prises en compte.

Cette page comprend les sections suivantes:

- **Host Name et Domain Name, page 28**
- **LAN Setting (adresse IP et sous-réseaux du périphérique), page 29**
- **WAN Setting (connexion Internet), page 32**
- **DMZ Setting, page 33**

Host Name et Domain Name

Certains fournisseurs d'accès Internet requièrent que vous attribuiez un nom d'hôte et un nom de domaine pour identifier votre routeur sur leur réseau. Des valeurs par défaut sont fournies, mais vous pouvez les modifier si vous le souhaitez.

- **Host Name:** gardez le paramètre par défaut ou saisissez le nom d'hôte spécifié par votre FAI.
- **Domain Name:** gardez le paramètre par défaut ou saisissez le nom de domaine spécifié par votre FAI.

IP Mode

Choisissez le type d'adressage à utiliser sur votre réseau:

- **IPv4 Only—**Utilisez uniquement l'adressage IPv4.
- **Dual-Stack IP—**Utilisez l'adressage IPv4 et IPv6. Après avoir activé cette option en enregistrant les paramètres sur cette page, vous pouvez configurer les adresses IPv4 et IPv6 pour les paramètres LAN, WAN et DMZ sur cette page.

LAN Setting (adresse IP et sous-réseaux du périphérique)

Les paramètres LAN par défaut sont généralement suffisants pour la plupart des petites entreprises, mais si cela est nécessaire, vous pouvez modifier l'adresseIP LAN du routeur et activer plusieurs sous-réseaux.

- **Modification de l'adresseIP du périphérique, page 29**
- **Enabling multiple subnets (IPv4 uniquement), page 31**

REMARQUE Si vous avez activé Dual-Stack IP pour le mode IP, cliquez sur l'onglet IPv6 pour configurer les adresses IPv6.

Modification de l'adresseIP du périphérique

STEP 1 Saisissez les informations suivantes:

- **Pour IPv4 :** cliquez sur l'onglet **IPv4**, puis renseignez les champs **Device IP Address** et **Subnet Mask**. L'adresse IP par défaut est 192.168.1.1 et le masque de sous-réseau par défaut est 255.255.255.0.
  Remarque: l'adresse MAC du routeur apparaît également dans cette section. Cette valeur ne peut pas être modifiée.
- **Pour IPv6 :** cliquez sur l'onglet **IPv6**, puis renseignez les champs **IPv6 Address** et **Prefix Length**. L'adresseIP par défaut est fc00::1 tandis que la longueur du préfixe par défaut est 7. L'onglet IPv6 est seulement disponible si l'option **Dual-Stack IP** est activée dans la section *IP Mode*. Si vous modifiez le paramètre IP Mode, vous devez enregistrer les paramètres avant de continuer.

  Remarque: Pour configurer les préfixesdes adresses IPv6 globales pour vos périphériques LAN, accédez à la section *WAN Settings*, cliquez sur l'onglet **IPv6**, puis cliquez sur l'icône **Edit** correspondant à l'interface WAN. Saisissez ensuite l'adresse LAN IPv6. Pour plus d'informations, voir **WAN Setting (connexion Internet), page 32**.

STEP 2 Cliquez sur **Save** pour enregistrer vos modifications ou sur **Cancel** pour les annuler.

Après avoir cliqué sur Save, une fenêtre contextuelle affiche un rappel indiquant que vous devez utiliser la nouvelle adresseIP du périphérique pour lancer l'utilitaire de configuration. Cliquez sur **OK** pour fermer le message et poursuivre la modification de l'adresseIP ou sur **Cancel** pour fermer le message sans appliquer les modifications.

STEP 3 Libérez et renouvelez l'adresseIP de votre ordinateur. Vous devriez normalement recevoir une nouvelle adresseIP située dans la nouvelle plage DHCP du routeur.

Remarques:

- *Pour libérer et renouveler votre adresse dans Windows :* À partir du menu Démarrer, ouvrez la fenêtre *Connexions réseau*. Cliquez avec le bouton droit sur la connexion et choisissez **Disable**. Cliquez à nouveau avec le bouton droit et activez la connexion. Pour vérifier, cliquez avec le bouton droit et choisissez **Status**. Cliquez ensuite sur l'onglet **Support** pour afficher l'adresse IP affectée.
- Par défaut, le routeur est un serveur DHCP qui attribue des adressesIP dynamiquement à tous les périphériques connectés. Si, par exemple, vous choisissez 192.168.15.1 comme l'adresse IP du périphérique, les périphériques recevront des adresses IP dans la plage 192.168.2.x.
- Par défaut, un ordinateur Windows reçoit également une adresseIP dynamique.
- Si vous avez préalablement désactivé le serveur DHCP du routeur ou défini une adresseIP statique sur l'ordinateur, vous devez configurer une nouvelle adresseIP statique dans la nouvelle plage.

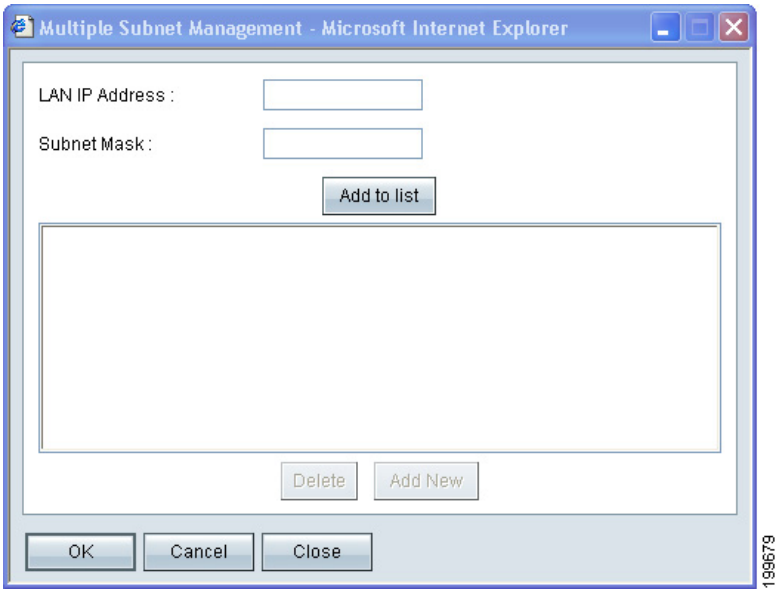
STEP 4 Pour vous reconnecter à l'utilitaire de configuration, saisissez la nouvelle adresseIP DU périphérique dans la barre d'adresse de votre navigateur.

Enabling multiple subnets (IPv4 uniquement)

En général, les routeurs de la gamme RV0xx Cisco sont utilisés comme routeurs d'accès, avec un seul sous-réseau LAN. Par défaut, le pare-feu est préconfiguré pour refuser l'accès LAN si l'adresseIP source est sur un sous-réseau différent de celui de l'adresseIP LAN du routeur. Cependant, vous pouvez activer plusieurs sous-réseaux pour permettre à ce routeur de fonctionner comme périphérique de périmètre fournissant la connectivité Internet à divers sous-réseaux de votre réseau LAN.

STEP 1 Dans l'onglet IPv4, cochez la case **Enable Multiple Subnet** pour activer cette fonctionnalité. Décochez la case pour désactiver cette option.

STEP 2 Cliquez sur **Add/Edit** pour créer ou modifier les sous-réseaux. Après avoir cliqué sur le bouton, la fenêtre *Multiple Subnet Management* s'affiche.



STEP 3 Dans la fenêtre contextuelle, ajoutez ou modifiez les entrées nécessaires.

- **Pour ajouter un nouveau sous-réseau:** saisissez une adresseIP LAN et un masque de sous-réseau. Cliquez sur **Add to list**. L'adresseIP et le masque de sous-réseau s'affichent dans la liste. Répétez cette étape autant de fois que nécessaire pour ajouter d'autres sous-réseaux.

Exemples:

- Deux sous-réseaux: si le routeur a l'adresseIP LAN 192.168.1.1 avec le masque de sous-réseau 255.255.255.0, vous pouvez configurer un deuxième sous-réseau avec l'adresseIP LAN 192.168.2.1 et le masque de sous-réseau 255.255.255.0.
- Quatre sous-réseaux: si le routeur a l'adresseIP LAN 192.168.1.1 et le masque de sous-réseau 255.255.255.192, vous pouvez créer trois sous-réseaux avec les adressesIP 192.168.2.65, 192.168.2.129 et 192.168.2.193 et le même masque de sous-réseau 255.255.255.192.

- **Pour ajouter un autre sous-réseau:** saisissez les informations, puis cliquez sur **Add to list**.
- **Pour modifier un sous-réseau:** cliquez sur le sous-réseau dans la liste. Les valeurs existantes apparaissent dans les champs de texte. Saisissez les nouvelles informations, puis cliquez sur **Update**. Si vous ne voulez pas modifier le sous-réseau sélectionné, vous pouvez cliquer sur **Add New** pour effacer les champs de texte.
- **Pour supprimer un sous-réseau:** dans la liste, cliquez sur le sous-réseau, puis cliquez sur **Delete**.

STEP 4 Lorsque vous avez fini de spécifier les paramètres dans la fenêtre *Multiple Subnet*, cliquez sur **OK** pour enregistrer vos modifications ou sur **Cancel** pour les annuler.

WAN Setting (connexion Internet)

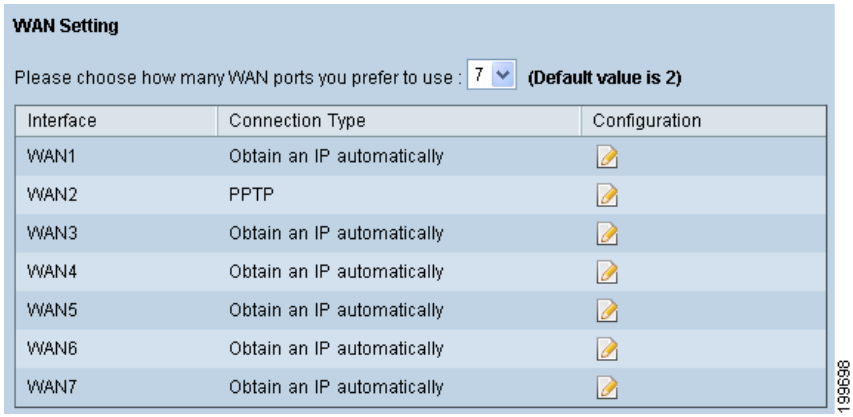
Le routeur est préconfiguré avec des paramètres par défaut suffisants pour la plupart des réseaux. Cependant, des paramètres spéciaux peuvent être requis par votre fournisseur d'accès Internet (FAI) ou par votre fournisseur de large bande (DSL ou câble). Reportez-vous aux informations de configuration fournies par votre FAI.

REMARQUE Vous pouvez également configurer votre connexion Internet à l'aide de l'assistant Basic Setup Wizard. Dans l'arborescence de navigation, cliquez sur **Wizard**. Dans la section *Basic Setup*, cliquez sur **Launch Now**.

Le tableau *WAN Setting* affiche les paramètres existants de chaque interface, tels que DMZ, WAN1 et WAN2. Les interfaces répertoriées dépendent du modèle du routeur et des paramètres spécifiés pour les ports, notamment pour la DMZ/Internet (tous les modèles) et les ports à double fonction (Cisco RV016).

Procédez comme suit, le cas échéant.

- **Pour configurer le réseau WAN avec l'adressage IPv6 :** cliquez sur l'onglet **IPv6**. Puis effectuez les tâches mentionnées ci-dessous.
  Remarque: l'onglet IPv6 est uniquement disponible si **Dual-Stack IP** est activé dans la section *IP Mode*. Si vous modifiez le paramètre IP Mode, vous devez enregistrer les paramètres avant de continuer.
- **Pour modifier le nombre de ports WAN (Cisco RV016 uniquement):** utilisez la liste déroulante pour choisir le nombre de ports WAN à activer. La valeur 2 est sélectionnée par défaut. Si vous configurez des ports WAN supplémentaires, des ports à double fonction sont alors utilisés.



- **Pour modifier les paramètres WAN :** Si vous n'avez pas enregistré des modifications dans la page *Network*, cliquez sur **Save** pour enregistrer vos paramètres avant de continuer. Pour accéder à l'interface à modifier, cliquez sur l'icône **Edit**. La page *Edit WAN Connection* apparaît. Pour obtenir plus d'informations, reportez-vous à la **Modification d'une connexion WAN, page 35**.

DMZ Setting

Sur les routeurs Cisco RV042, RV042G et RV082, vous pouvez configurer le port Internet/DMZ pour une utilisation en tant que DMZ (zone démilitarisée ou zone de démarcation). Le routeur Cisco RV016 dispose d'un port DMZ dédié. Grâce à la connexion DMZ, le trafic Internet peut accéder aux hôtes spécifiés de votre réseau, notamment les serveurs FTP et les serveurs Web. Le reste de vos ressources réseau reste privé.

Cette fonctionnalité requiert une adresseIP routable publiquement pour chaque hôte de la DMZ. Vous pouvez contacter votre FAI pour obtenir une adresseIP supplémentaire consacrée à ce but.

REMARQUE

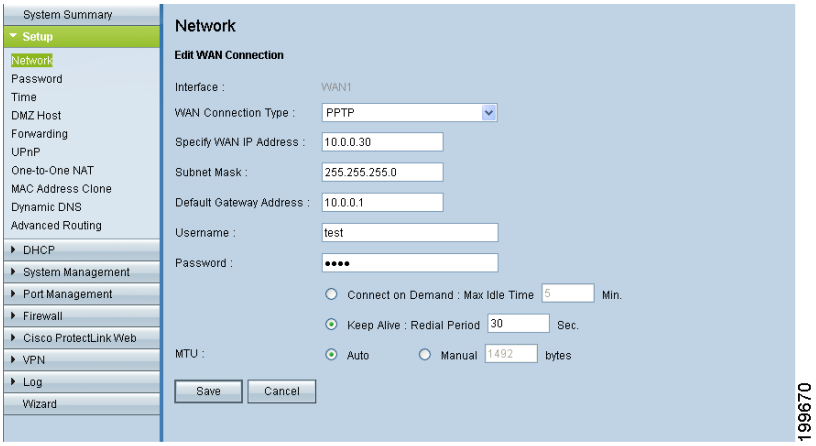
- L'utilisation de la DMZ est souhaitée et constitue, dans la mesure du possible, une solution préférable à l'utilisation de serveurs LAN publics ou à la connexion de ces serveurs à des ports WAN, qui n'offrent aucune protection aux serveurs et qui ne sont pas accessibles par les utilisateurs du réseau LAN.
- Chacun des serveurs de la DMZ nécessite une adresseIP Internet publique unique. Votre FAI devrait normalement être en mesure de fournir ces adresses, ainsi que les informations nécessaires à la configuration des serveurs Internet publics. Si vous prévoyez d'utiliser le paramètre DMZ, contactez votre FAI pour obtenir des informations concernant les adressesIP statiques. Si votre FAI fournit une seule adresseIP statique ou plusieurs adressesIP dynamiques, nous vous recommandons d'utiliser la fonctionnalité d'hôte DMZ. Reportez-vous à **Configuration d'un hôte DMZ, page 45**.

Procédez comme suit, le cas échéant.

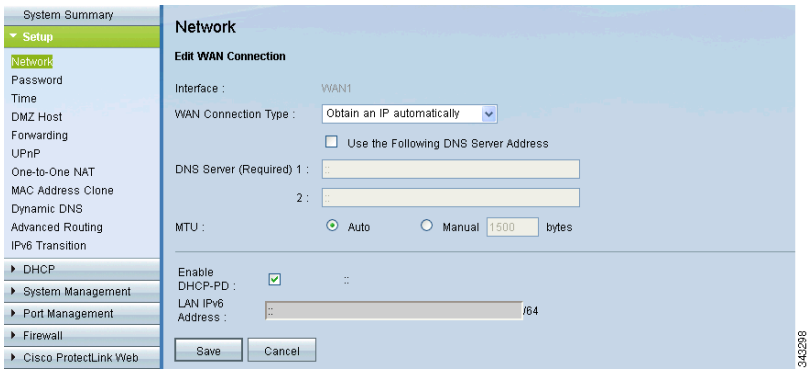
- **Pour configurer le réseau DMZ avec l'adressage IPv6:** cliquez sur l'onglet **IPv6**. Puis effectuez les autres tâches de cette section.
  Remarque: l'onglet IPv6 est uniquement disponible si **Dual-Stack IP** est activé dans la section *IP Mode*. Si vous modifiez le paramètre IP Mode, vous devez enregistrer les paramètres avant de continuer.
- **Pour activer DMZ sur le port DMZ/Internet (Cisco RV042, RV042G et RV082 uniquement):** cochez a case **Enable DMZ** pour activer cette fonctionnalité. Ensuite, modifiez les paramètres DMZ, comme décrit ci-après. Si vous souhaitez au contraire utiliser le port comme port WAN, décochez la case, et veillez à configurer les paramètres WAN de la page *Dual WAN*. (Reportez-vous à **Configuration des connexions WAN et Multi-WAN, page 76**.)
- **Pour modifier les paramètres DMZ :** cliquez sur l'icône **Edit** pour ouvrir la page *Edit DMZ Connection*. Pour obtenir plus d'informations, reportez-vous à la **Modification d'une connexion DMZ, page 40**. Si vous n'avez pas enregistré vos paramètres, une mise en garde s'affiche. Cliquez sur **OK** pour enregistrer vos paramètres ou sur **Cancel** pour fermer cette fenêtre sans faire d'enregistrement.

Modification d'une connexion WAN

Modification d'une connexion WAN avec l'adressage IPv4



Modification d'une connexion WAN avec l'adressage IPv6



La page *Edit WAN Connection* apparaît dès que vous cliquez sur une icône **Edit** dans la section *WAN Settings* de la page *Network*. Saisissez les informations qui vous ont été communiquées par votre fournisseur d'accès à Internet (FAI).

REMARQUE Avant de quitter cette page, cliquez sur **Save** pour enregistrer les paramètres ou sur **Cancel** pour les annuler. Les modifications non enregistrées ne sont pas prises en compte.

- **Interface :** le port WAN sélectionné apparaît. Il n'est pas possible de modifier cet identifiant.
- **WAN Connection Type :** sélectionnez un type de connexion, comme décrit ci-dessous.
  - **Obtain an IP Automatically :** sélectionnez cette option si votre fournisseur d'accès à Internet attribue une adresseIP de manière dynamique. La plupart des abonnés aux modems-câbles utilisent, par exemple, ce type de connexion. Votre fournisseur d'accès à Internet définit les paramètres, notamment l'adresseIP du serveur DNS. Si vous souhaitez spécifier un serveur DNS, cochez la case **Use the Following DNS Server Addresses**. Saisissez ensuite une adresseIP dans la zone **DNS Server (Required)1**. Vous pouvez éventuellement saisir un second serveur DNS. La première entrée DNS disponible est utilisée.
  - **Static IP :** sélectionnez cette option si votre fournisseur d'accès à Internet a attribué une adresseIP permanente à votre compte. Saisissez ensuite les paramètres spécifiés par votre fournisseur d'accès à Internet:

    Specify WAN IP Address : adresseIP externe que votre fournisseur d'accès à Internet a attribuée à votre compte.

    Subnet Mask (IPv4) : masque de sous-réseau spécifié par votre fournisseur d'accès à Internet.

    Prefix Length (IPv6) : longueur du préfixe spécifiée par votre fournisseur d'accès à Internet.

    Default Gateway Address : adresseIP de la passerelle par défaut.

    DNS Server (Required) 1 : adresseIP du serveur DNS spécifié. Saisissez éventuellement un second serveur DNS. La première entrée DNS disponible est utilisée.
  - **PPPoE (Point-to-Point Protocol over Ethernet) :** sélectionnez cette option si votre fournisseur d'accès à Internet utilise le protocole PPPoE pour établir des connexions à Internet (ce qui est généralement le cas

des lignes ADSL). Saisissez ensuite les paramètres spécifiés par votre fournisseur d'accès à Internet:

Username et **Password :** saisissez le nom d'utilisateur et le mot de passe du compte de votre fournisseur d'accès à Internet. Le nombre maximal de caractères est fixé à60.

Connect on Demand : cette fonctionnalité peut être utile si vous êtes facturé en fonction de la durée de connexion à Internet. Lorsque cette fonctionnalité est activée, la connexion prend fin après une période d'inactivité spécifiée (Max Idle Time). Dès que vous tentez d'accéder à nouveau à Internet, le routeur rétablit automatiquement la connexion. Si vous activez cette fonctionnalité, saisissez également la durée **Max Idle Time**, qui correspond au nombre de minutes pendant lesquelles la connexion peut être inactive; lorsque cette limite est atteinte, la connexion prend fin. Le délai d'inactivité maximal par défaut est de 5minutes.

Keep Alive : cette fonctionnalité permet de garantir que votre routeur est toujours connecté à Internet. Lorsque cette fonctionnalité est activée, le routeur garde cette connexion active en envoyant régulièrement quelques paquets de données. Cette option permet de garder votre connexion active indéfiniment, même si elle est inactive dans les faits. Si vous activez cette fonctionnalité, définissez également la valeur **Redial Period** pour spécifier la fréquence à laquelle le routeur doit vérifier votre connexion Internet. La période par défaut est de 30secondes.

- **PPTP (Point-to-Point Tunneling Protocol) :** sélectionnez cette option si votre fournisseur d'accès à Internet l'exige. PPTP est un service utilisé en Europe, en Israël et dans d'autres pays.

  Specify WAN IP Address : adresseIP externe que votre fournisseur d'accès à Internet a attribuée à votre compte.

  Subnet Mask : masque de sous-réseau spécifié par votre fournisseur d'accès à Internet.

  Default Gateway Address : adresseIP de la passerelle par défaut.

  Username et **Password :** saisissez le nom d'utilisateur et le mot de passe du compte de votre fournisseur d'accès à Internet. Le nombre maximal de caractères est fixé à60.

  Connect on Demand : cette fonctionnalité peut être utile si vous êtes facturé en fonction de la durée de connexion à Internet. Lorsque cette fonctionnalité est activée, la connexion prend fin après une période d'inactivité spécifiée (Max Idle Time). Dès que vous tentez d'accéder à

nouveau à Internet, le routeur rétablit automatiquement la connexion. Si vous activez cette fonctionnalité, saisissez également la durée **Max Idle Time**, qui correspond au nombre de minutes pendant lesquelles la connexion peut être inactive; lorsque cette limite est atteinte, la connexion prend fin. Le délai d'inactivité maximal par défaut est de 5minutes.

Keep Alive : cette fonctionnalité permet de garantir que votre routeur est toujours connecté à Internet. Lorsque cette fonctionnalité est activée, le routeur garde cette connexion active en envoyant régulièrement quelques paquets de données. Cette option permet de garder votre connexion active indéfiniment, même si elle est inactive dans les faits. Si vous activez cette fonctionnalité, définissez également la valeur **Redial Period** pour spécifier la fréquence à laquelle le routeur doit vérifier votre connexion Internet. La période par défaut est de 30secondes.

- **Transparent Bridge :** sélectionnez cette option si vous utilisez ce routeur pour connecter deux segments de réseau. Une seule interface WAN peut être configurée comme pont transparent.

  Specify WAN IP Address : adresseIP externe que votre fournisseur d'accès à Internet a attribuée à votre compte.

  Subnet Mask : masque de sous-réseau spécifié par votre fournisseur d'accès à Internet.

  Default Gateway Address : adresseIP de la passerelle par défaut.

  DNS Server (Required) 1 : adresseIP du serveur DNS spécifié. Saisissez éventuellement un second serveur DNS. La première entrée DNS disponible est utilisée.

  Internal LAN IP Range : plage d'adressesIP LAN interne reliée par un pont. Les réseaux WAN et LAN du pont transparent partagent le même sous-réseau.

- **MTU :** définissez la valeur **Taille maximum de l'unité de transfert (MTU)** en octets (voir le Glossaire). Sauf indication contraire de votre fournisseur d'accès à Internet, Cisco recommande d'utiliser le paramètre par défaut, **Auto**. Pour spécifier une autre valeur, sélectionnez **Manual**, puis saisissez la taille en octets.
- **Enabled DHCP-PD :** cochez cette case pour activer le processus client DHCPv6 et autoriser une demande de délégation de préfixe via l'interface sélectionnée. Cette option est généralement utilisée lorsque votre fournisseur d'accès à Internet est capable d'envoyer des préfixes LAN via l'option DHCPv6. Si votre fournisseur d'accès à Internet ne prend pas en

charge cette option, vous pouvez configurer manuellement un préfixe LAN en saisissant l'adresse LANIPv6 ci-dessous.

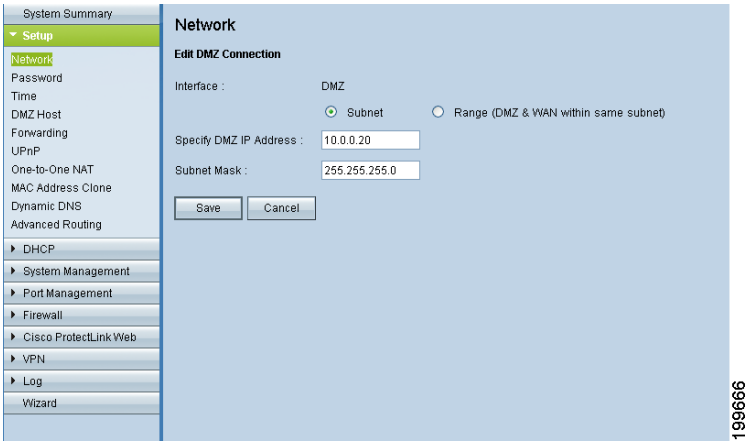
Remarque : si la fonctionnalité DHCP-PD est activée, l'adressage manuel LAN IPv6 ci-dessous est désactivé et inversement.

- **LAN IPv6 Address :** cette option permet de saisir le préfixe IPv6 global attribué par votre FAI pour vos périphériques LAN, le cas échéant. Pour en savoir plus à ce sujet, renseignez-vous auprès de votre FAI.

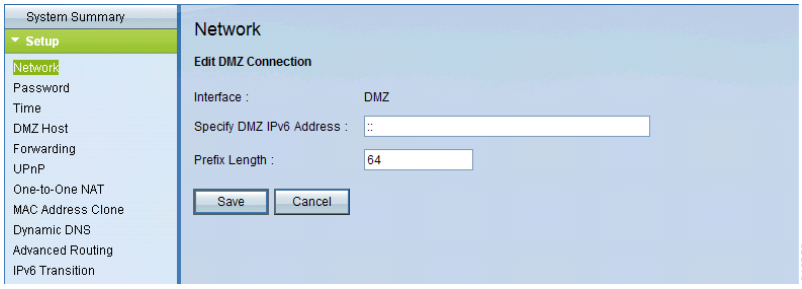
Modification d'une connexion DMZ

Servez-vous de la page *Edit DMZ Connection* pour définir les paramètres de votre connexion DMZ. L'interface DMZ est activée par défaut.

IPv4



IPv6



La page *Edit DMZ Connection* apparaît dès que vous cliquez sur l'icône **Edit** dans la section *DMZ Setting* de la page *Network*.

REMARQUE Avant de quitter cette page, cliquez sur **Save** pour enregistrer les paramètres ou sur **Cancel** pour les annuler. Les modifications non enregistrées ne sont pas prises en compte.

Si vous utilisez l'adressage IPv4, saisissez les informations suivantes:

- **Subnet :** sélectionnez cette option pour placer la zone démilitarisée (DMZ) sur un sous-réseau différent du réseau WAN (paramètre par défaut). Saisissez l'adresseIP et le masque de sous-réseau pour la zone démilitarisée (DMZ).

- **Range :** sélectionnez cette option pour placer la zone démilitarisée (DMZ) sur le même sous-réseau que le réseau WAN. Saisissez la plage d'adressesIP à réserver au port DMZ.

Si vous utilisez l'adressage IPv6, saisissez les informations suivantes:

- **Specify DMZ IPv6 Address :** saisissez une adresse IPv6 pour votre DMZ. Remplacez le double symbole des deux points par défaut (**::)** par une adresse IPv6 valide pour votre DMZ.
- **Prefix Length :** saisissez la longueur de préfixe. La valeur par défaut est64.

Changement du nom d'utilisateur et du mot de passe de l'administrateur

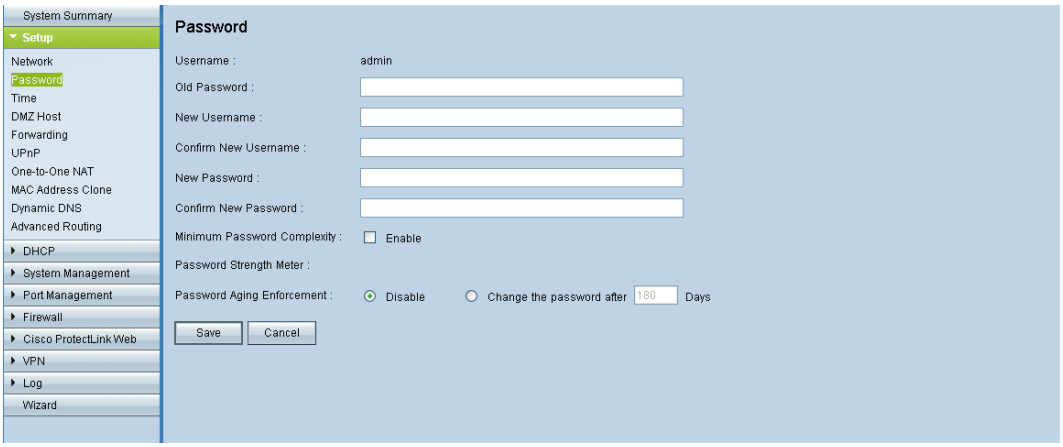
Utilisez la page *Setup > Password* pour mettre à jour le nom d'utilisateur et le mot de passe de l'administrateur. Vous pouvez conserver le nom d'utilisateur par défaut (admin), si vous le souhaitez. Toutefois, Cisco vous recommande vivement de modifier le mot de passe par défaut (admin) et de le remplacer par un mot de passe difficile à deviner.

ATTENTION Il n'est pas possible de récupérer ce mot de passe si vous l'oubliez ou le perdez. Le cas échéant, vous devez réinitialiser le routeur afin qu'il retrouve ses paramètres par défaut définis en usine. Sachez cependant que toutes les modifications que vous avez apportées à votre configuration seront perdues.

REMARQUE

- Vous devez modifier le mot de passe de l'administrateur si vous activez l'accès distant sur la page *Firewall > General*.
- Avant de quitter cette page, cliquez sur **Save** pour enregistrer les paramètres ou sur **Cancel** pour les annuler. Une fois que vous avez modifié le nom d'utilisateur ou le mot de passe, vous êtes invité à vous connecter à l'aide des nouvelles informations d'identification, lorsque vous sélectionnez une option dans l'arborescence.

Pour ouvrir cette page: cliquez sur **Setup> Password** dans l'arborescence.



- **Old Password:** saisissez votre ancien mot de passe. Le mot de passe par défaut est **admin**.
- **New Username:** saisissez un nouveau nom d'utilisateur, s'il y a lieu. Pour conserver le nom d'utilisateur existant, ne renseignez pas ce champ.
- **Confirm New Username:** pour confirmer votre choix, saisissez de nouveau le nom d'utilisateur, tel que vous l'avez entré dans le champ précédent.
- **New Password:** saisissez un nouveau mot de passe pour le routeur. Vous pouvez inclure des symboles et des caractères alphanumériques, mais pas d'espaces.
- **Confirm New Password:** pour confirmer votre choix, saisissez de nouveau le mot de passe, tel que vous l'avez entré dans le champ précédent. Un message d'erreur s'affiche si les deux mots de passe ne concordent pas.
- **Minimum Password Complexity:** cochez la case **Enable** si vous souhaitez appliquer la règle de complexité du mot de passe et activer la fonctionnalité de mesure de la puissance du mot de passe. Cette option est activée par défaut et son utilisation est vivement recommandée.

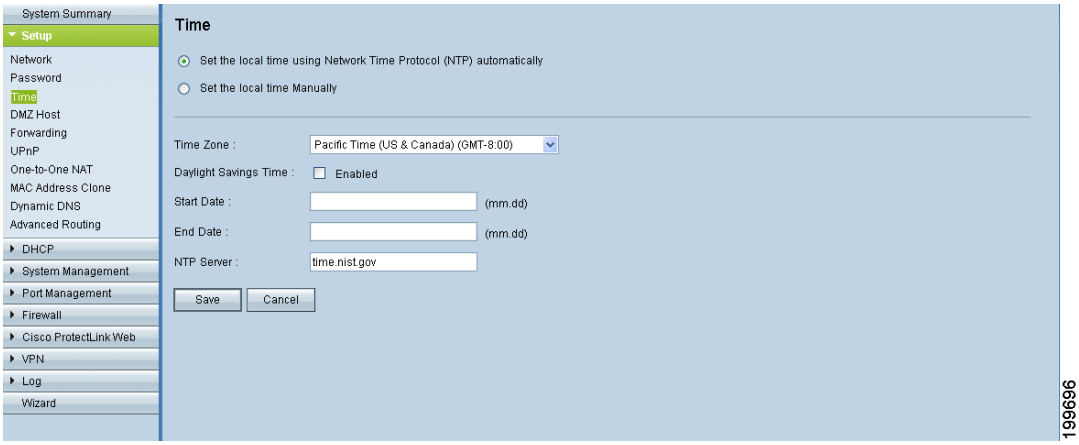
  Lorsque l'option Minimum Password Complexity est activée, le mot de passe doit respecter certaines conditions énumérées ci-dessous. Votre saisie est validée lorsque vous cliquez sur le bouton Save.

  - Doit inclure au moins 8caractères.
  - Ne doit pas être identique au nom d'utilisateur.
  - Ne doit pas être identique au mot de passe actuel.
  - Doit contenir des caractères provenant d'au moins 3 des 4catégories suivantes: lettres majuscules, lettres minuscules, chiffres et caractères spéciaux que l'on trouve sur un clavier standard.
- **Password Strength Meter:** si vous activez l'option Minimum Password Complexity, cette option indique la puissance du mot de passe, en fonction des règles de complexité définies. Des barres colorées s'affichent à mesure que vous saisissez un mot de passe. L'échelle va du rouge (inacceptable) au vert (fort), en passant par le jaune (acceptable).
- **Password Aging Enforcement:** choisissez **Disable** si vous ne voulez pas que le mot de passe expire. Sélectionnez **Change the password after** si vous souhaitez que le mot de passe arrive à expiration après le nombre de **jours** spécifié (la valeur par défaut est180).

Réglage de l'heure système

Utilisez la page *Setup > Time* pour spécifier l'heure système du réseau. Le routeur utilise les paramètres horaires pour horodater les événements consignés pour appliquer des règles d'accès et des filtres de contenu automatiques et pour effectuer d'autres activités, à des fins internes. Vous pouvez configurer le routeur pour qu'il reçoive les paramètres horaires locaux automatiquement à partir d'un serveur, ou vous pouvez saisir l'heure locale manuellement.

Pour ouvrir cette page: cliquez sur **Setup> Time** dans l'arborescence.



REMARQUE Avant de quitter cette page, cliquez sur **Save** pour enregistrer vos paramètres ou sur **Cancel** pour les annuler. Les modifications non enregistrées ne sont pas prises en compte.

Sélectionnez l'une des options suivantes pour régler l'heure, puis saisissez les informations requises.

- **Set the local time using Network Time Protocol (NTP) automatically:** sélectionnez cette option pour permettre au routeur de recevoir les paramètres horaires automatiquement, à partir d'un serveur. Définissez ensuite les paramètres suivants:
  - **Time Zone :** sélectionnez votre fuseau horaire. La valeur par défaut est **(GMT-08:00) Pacific Time (US & Canada); Tijuana**.
  - **Daylight Saving:** pour régler automatiquement l'heure d'été, sélectionnez **Enabled**. Dans le champ **Start Date**, saisissez la date de début du passage à l'heure d'été (jour et mois). Utilisez le format mm.jj, comme dans 6.25, pour désigner le 25juin. Saisissez également la **date de fin** dans le même format.

- **NTP Server :** saisissez l'adresse URL ou l'adresseIP du serveur NTP. La valeur par défaut est *time.nist.gov*.

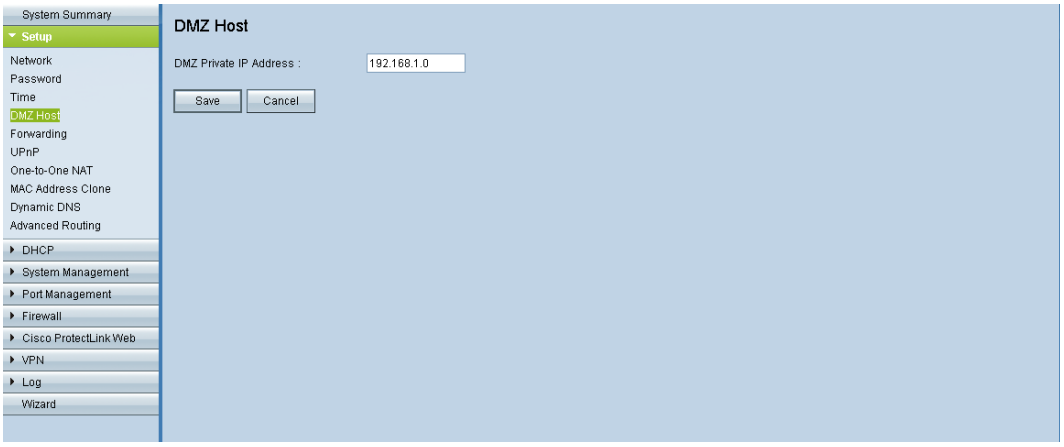
▪ **Set the local time Manually:** choisissez cette option si vous voulez définir vous-même l'heure locale. Saisissez ensuite les informations suivantes:

- **Date:** saisissez la date actuelle au format aaaa.mm.jj, comme dans 2010.06.25, pour désigner le 25juin 2010.
- **Hours, Minutes, Seconds:** saisissez l'heure actuelle au format hh:mm:ss, comme dans 15:17:00, pour indiquer 15h17.

Configuration d'un hôte DMZ

Utilisez la page *Setup > DMZ Host* pour permettre à un hôte du réseau local d'être exposé sur Internet, pour utiliser des services de vidéoconférence ou de jeu. L'accès à l'hôte DMZ depuis Internet peut être restreint davantage via l'utilisation de règles d'accès à travers un pare-feu.

Pour ouvrir cette page: cliquez sur **Setup> DMZ Host** dans l'arborescence.



Saisissez l'adresseIP du périphérique réseau que vous souhaitez utiliser comme hôte DMZ.

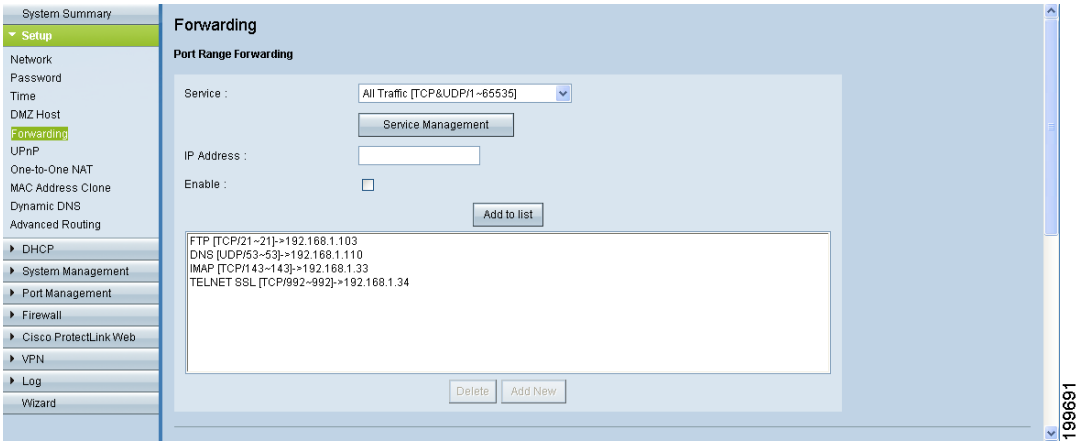
REMARQUE Avant de quitter cette page, cliquez sur **Save** pour enregistrer les paramètres ou sur **Cancel** pour les annuler. Les modifications non enregistrées ne sont pas prises en compte.

Configuration du déclenchement et de la redirection de port

Utilisez la page *Setup > Forwarding* si vous devez configurer un accès public à des services proposés sur des ordinateurs qui sont connectés aux ports du réseau local. La redirection de port ouvre une plage de ports ou un port spécifié pour un service, tel que FTP. Le déclenchement de port ouvre une plage de ports pour des services, tels que les jeux sur Internet, qui utilisent d'autres ports pour communiquer entre le serveur et l'hôte LAN. Cette page comporte les sections suivantes:

- **Port Range Forwarding, page 46**
- **Port Triggering, page 49**

Pour ouvrir cette page: cliquez sur **Setup > Forwarding** dans l'arborescence.



REMARQUE Avant de quitter cette page, cliquez sur **Save** pour enregistrer vos paramètres ou sur **Cancel** pour les annuler. Les modifications non enregistrées ne sont pas prises en compte.

Port Range Forwarding

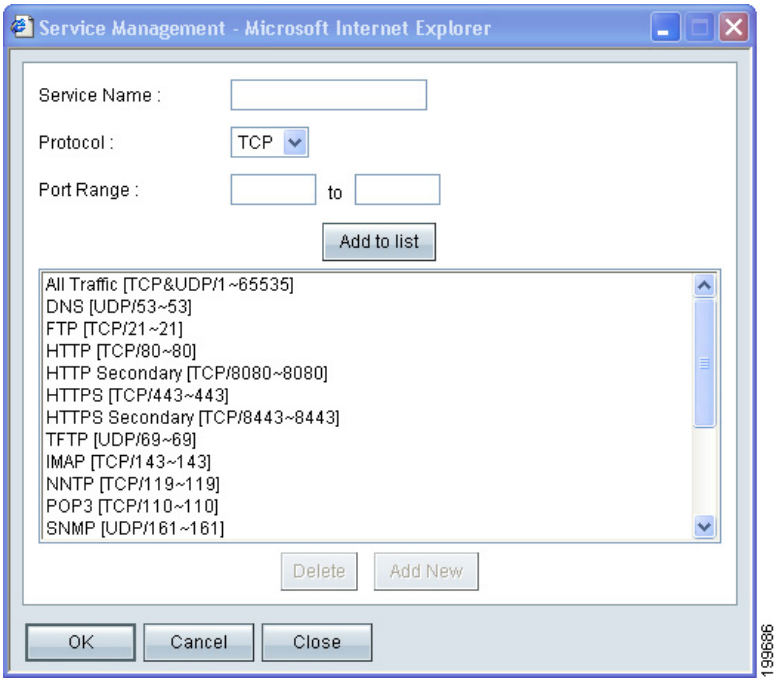
La redirection de port permet de configurer des services publics sur votre réseau. Lorsque des utilisateurs lancent certaines requêtes depuis Internet sur votre réseau, le routeur peut les transférer vers des ordinateurs équipés pour leur traitement. Par exemple, si vous configurez le numéro de port80 (HTTP) afin qu'il soit transféré à l'adresseIP 192.168.1.2, toutes les requêtes HTTP provenant d'utilisateurs externes sont transférées à l'adresse 192.168.1.2.

Vous pouvez utiliser cette fonctionnalité pour établir un serveur Web ou FTP via une passerelleIP. Veillez à saisir une adresseIP valide. (Vous devrez peut-être établir une adresseIP statique afin d'exécuter correctement un serveur Internet.) Pour plus de sécurité, les utilisateurs d'Internet sont en mesure de communiquer avec le serveur, bien qu'ils ne soient pas réellement connectés. Les paquets sont simplement transférés par l'intermédiaire du routeur.

- **Pour ajouter une entrée à la liste:** saisissez les informations suivantes, puis cliquez sur **Add to list**.
  - **Service:** sélectionnez le service. Si un service particulier n'est pas répertorié dans la liste, vous pouvez l'ajouter. Pour obtenir des détails, reportez-vous à **Ajout d'un service, page 48**.
  - **IP Address:** saisissez l'adresseIP LAN du serveur auquel vous souhaitez que les utilisateurs d'Internet puissent accéder.
  - **Enable:** cochez la case pour activer l'entrée de redirection de plage de ports correspondante.
- **Pour ajouter une nouvelle entrée:** saisissez les informations, puis cliquez sur **Add to list**.
- **Pour modifier une entrée de la liste:** cliquez sur l'entrée à modifier. Les informations apparaissent dans les champs de texte. Apportez les modifications voulues, puis cliquez sur **Update**. Si aucune modification n'est nécessaire, cliquez sur **Add New** pour désélectionner l'entrée et effacer le contenu des champs de texte.
- **Pour supprimer une entrée de la liste:** cliquez sur l'entrée à supprimer, puis sur **Delete**. Pour sélectionner un bloc d'entrées, cliquez sur la première entrée, maintenez la touche **Maj** enfoncée, puis cliquez sur la dernière entrée du bloc. Pour sélectionner des entrées individuellement, maintenez la touche **Ctrl** enfoncée, tout en cliquant sur chacune des entrées en question. Pour annuler la sélection d'une entrée, maintenez la touche **Ctrl** enfoncée tout en cliquant sur l'entrée.
- **Pour afficher le tableau de plages de ports:** cliquez sur **View** en bas de la page. Sélectionnez **Port Range Forwarding** ou **Port Triggering**. Pour mettre à jour les informations, cliquez sur **Refresh**. Pour revenir à la page *Forwarding* , cliquez sur **Close**.

Ajout d'un service

Pour ajouter une nouvelle entrée à la liste *Service* ou pour modifier une entrée créée précédemment, cliquez sur **Service Management**. Si le navigateur Web affiche une mise en garde relative à la fenêtre contextuelle, autorisez le contenu bloqué.



Dans la fenêtre *Service Management*, ajoutez ou mettez à jour des entrées, selon vos besoins. Avant de fermer cette fenêtre, cliquez sur **OK** pour enregistrer vos paramètres ou sur **Cancel** pour les annuler. Les modifications non enregistrées ne sont pas prises en compte.

- **Pour ajouter un service à la liste:** saisissez les informations suivantes, puis cliquez sur **Add to list**. La liste peut comporter jusqu'à 30services.
  - **Service Name :** entrez une brève description.
  - **Protocol :** sélectionnez le protocole requis. Reportez-vous à la documentation du service que vous hébergez.
  - **Port Range :** saisissez la plage de ports requise.
- **Pour ajouter un nouveau service:** saisissez les informations, puis cliquez sur **Add to list**.

- **Pour modifier un service que vous avez créé:** cliquez sur le service dans la liste. Les informations apparaissent dans les champs de texte. Apportez les modifications voulues, puis cliquez sur **Update**. Si aucune modification n'est nécessaire, cliquez sur **Add New** pour désélectionner le service et effacer le contenu des champs de texte.
- **Pour supprimer un service de la liste:** cliquez sur l'entrée à supprimer. Pour sélectionner un bloc d'entrées, cliquez sur la première entrée, maintenez la touche **Maj** enfoncée, puis cliquez sur la dernière entrée du bloc. Pour sélectionner plusieurs entrées individuelles, maintenez la touche **Ctrl** enfoncée tout en cliquant sur les entrées. Cliquez sur **Delete**.

Port Triggering

Le déclenchement de port permet au routeur de contrôler les données sortantes à la recherche des numéros de port spécifiés. Lorsque les données demandées transitent de nouveau par le routeur, elles sont ainsi redirigées vers l'ordinateur approprié au moyen de l'adresse IP et des règles de mappage de ports.

Certains jeux ou applications Internet utilisent d'autres ports pour communiquer entre le serveur et l'hôte LAN. Lorsque vous souhaitez utiliser ces applications, saisissez le port de déclenchement (sortant) et l'autre port entrant dans le tableau *Port Triggering*. Le routeur redirige alors les paquets entrants vers l'hôte LAN spécifié.

Ajoutez ou modifiez les entrées, selon vos besoins. N'oubliez pas que les paramètres ne sont pas enregistrés tant que vous n'avez pas cliqué sur le bouton Save.

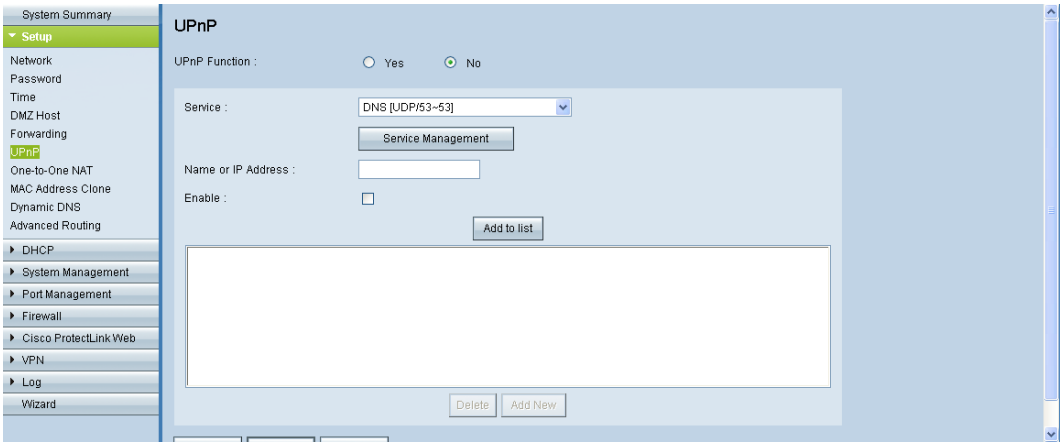
- **Pour ajouter une entrée à la liste:** saisissez les informations suivantes, puis cliquez sur **Add to list**. La liste peut comporter jusqu'à 30applications.
  - **Application Name :** saisissez le nom de l'application.
  - **Trigger Port Range:** saisissez les numéros de port de début et de fin de la plage de ports de déclenchement. Reportez-vous à la documentation de l'application.
  - **Incoming Port Range:** saisissez les numéros de port de début et de fin de la plage de ports entrants. Reportez-vous à la documentation de l'application.
  - **Enable:** cochez cette case pour activer le déclenchement de port pour l'application. Décochez-la pour désactiver l'application.
- **Pour ajouter une nouvelle entrée:** saisissez les informations, puis cliquez sur **Add to list**.

- **Pour modifier une entrée de la liste:** cliquez sur l'entrée à modifier. Les informations apparaissent dans les champs de texte. Apportez les modifications voulues, puis cliquez sur **Update**. Si aucune modification n'est nécessaire, cliquez sur **Add New** pour désélectionner l'entrée et effacer le contenu des champs de texte.
- **Pour supprimer une entrée de la liste:** cliquez sur l'entrée à supprimer, puis sur **Delete**. Pour sélectionner un bloc d'entrées, cliquez sur la première entrée, maintenez la touche **Maj** enfoncée, puis cliquez sur la dernière entrée du bloc. Pour sélectionner des entrées individuellement, maintenez la touche **Ctrl** enfoncée, tout en cliquant sur chacune des entrées en question. Pour annuler la sélection d'une entrée, maintenez la touche **Ctrl** enfoncée tout en cliquant sur l'entrée.
- **Pour afficher le tableau de plages de ports:** cliquez sur **View** en bas de la page. Sélectionnez **Port Range Forwarding** ou **Port Triggering**. Pour mettre à jour les informations, cliquez sur **Refresh**. Pour revenir à la page *Forwarding* , cliquez sur **Close**.

Configuration de la fonctionnalité Plug and Play universel (UPnP)

Utilisez la page *Setup > UPnP* pour activer la fonctionnalité Plug and Play universel (UPnP). Cette fonction permet à Windows de configurer automatiquement le routeur afin qu'il ouvre et ferme des ports aux applications Internet telles que les jeux ou la vidéoconférence.

Pour ouvrir cette page: cliquez sur **Setup> UPnP** dans l'arborescence.



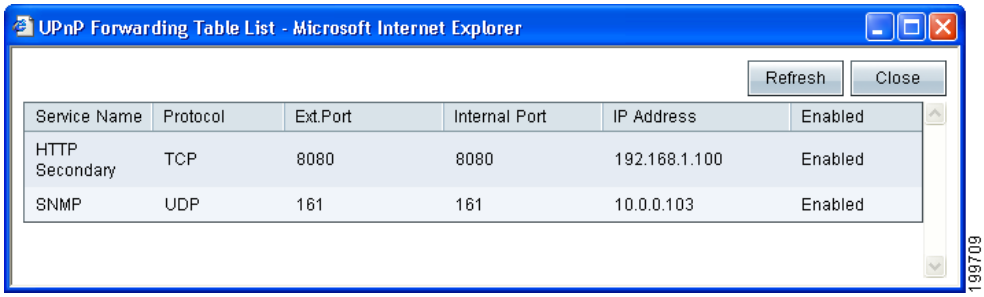
REMARQUE

- Par mesure de précaution, désactivez UPnP jusqu'à ce que vous ayez besoin de cette fonctionnalité pour vos applications.
- Avant de quitter cette page, cliquez sur **Save** pour enregistrer les paramètres ou sur **Cancel** pour les annuler. Les modifications non enregistrées ne sont pas prises en compte.

Pour activer la fonctionnalité UPnP, cliquez sur **Yes**. Pour désactiver cette fonctionnalité, cliquez sur **No**. Ajoutez ou modifiez les entrées, selon vos besoins.

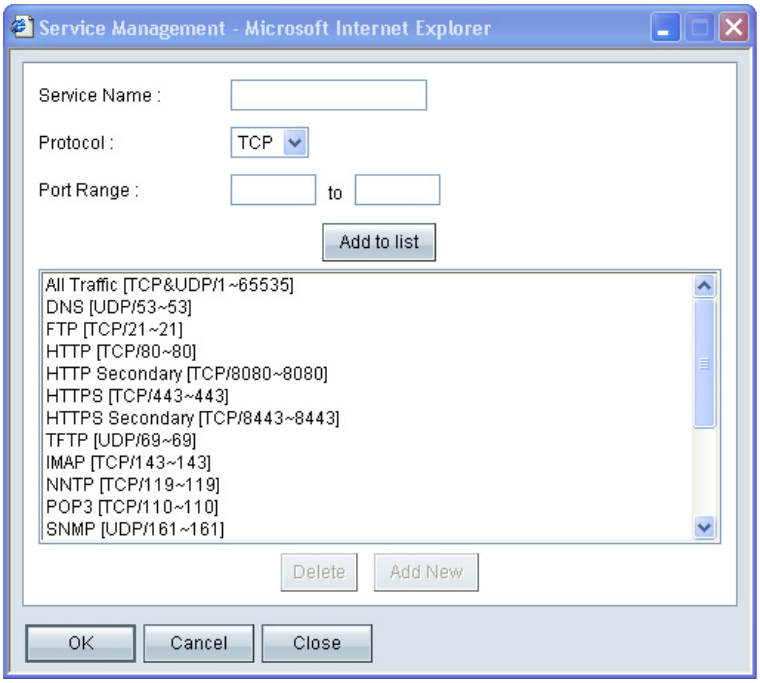
- **Pour ajouter une entrée à la liste:** saisissez les informations suivantes, puis cliquez sur **Add to list**. La liste peut comporter jusqu'à 30services.
  - **Service:** sélectionnez le service. Si un service particulier n'est pas répertorié dans la liste, vous pouvez l'ajouter. Reportez-vous à **Ajout d'un service, page 52**.
  - **Name or IP Address:** saisissez le nom ou l'adresseIP du périphérique UPnP.
  - **Enable:** sélectionnez **Enable** pour activer cette entrée UPnP.
- **Pour ajouter une nouvelle entrée:** saisissez les informations, puis cliquez sur **Add to list**.
- **Pour modifier une entrée de la liste:** cliquez sur l'entrée à modifier. Les informations apparaissent dans les champs de texte. Apportez les modifications voulues, puis cliquez sur **Update**. Si aucune modification n'est nécessaire, cliquez sur **Add New** pour désélectionner l'entrée et effacer le contenu des champs de texte.
- **Pour supprimer une entrée de la liste:** cliquez sur l'entrée à supprimer, puis sur **Delete**. Pour sélectionner un bloc d'entrées, cliquez sur la première entrée, maintenez la touche **Maj** enfoncée, puis cliquez sur la dernière entrée du bloc. Pour sélectionner des entrées individuellement, maintenez la touche **Ctrl** enfoncée, tout en cliquant sur chacune des entrées en question. Pour annuler la sélection d'une entrée, maintenez la touche **Ctrl** enfoncée tout en cliquant sur l'entrée.

  La liste *UPnP Forwarding Table List* affiche les données actuelles. Vous pouvez cliquer sur **Refresh** pour mettre à jour les données ou sur **Close** pour fermer la fenêtre contextuelle.
- **Pour afficher le tableau de redirection UPnP:** cliquez sur **View** en bas de la page. Pour mettre à jour les informations, cliquez sur **Refresh**. Pour revenir à la page *UPnP* , cliquez sur **Close**.



Ajout d'un service

Pour ajouter une nouvelle entrée à la liste *Service* ou pour modifier une entrée créée précédemment, cliquez sur **Service Management**. Si le navigateur Web affiche une mise en garde relative à la fenêtre contextuelle, autorisez le contenu bloqué.



Dans la fenêtre *Service Management*, ajoutez ou mettez à jour des entrées, selon vos besoins. Avant de fermer cette fenêtre, cliquez sur **OK** pour enregistrer vos paramètres ou sur **Cancel** pour les annuler. Les modifications non enregistrées ne sont pas prises en compte.

- **Pour ajouter un service à la liste:** saisissez les informations suivantes, puis cliquez sur **Add to list**. La liste peut comporter jusqu'à 30services.

- **Service Name :** entrez une brève description.
- **Protocol :** sélectionnez le protocole requis. Reportez-vous à la documentation du service que vous hébergez.
- **Port Range :** saisissez la plage de ports requise.

- **Pour ajouter un nouveau service:** saisissez les informations, puis cliquez sur **Add to list**.
- **Pour modifier un service que vous avez créé:** cliquez sur le service dans la liste. Les informations apparaissent dans les champs de texte. Apportez les modifications voulues, puis cliquez sur **Update**. Si aucune modification n'est nécessaire, cliquez sur **Add New** pour désélectionner le service et effacer le contenu des champs de texte.
- **Pour supprimer un service de la liste:** cliquez sur l'entrée à supprimer. Pour sélectionner un bloc d'entrées, cliquez sur la première entrée, maintenez la touche **Maj** enfoncée, puis cliquez sur la dernière entrée du bloc. Pour sélectionner plusieurs entrées individuelles, maintenez la touche **Ctrl** enfoncée tout en cliquant sur les entrées. Cliquez sur **Delete**.

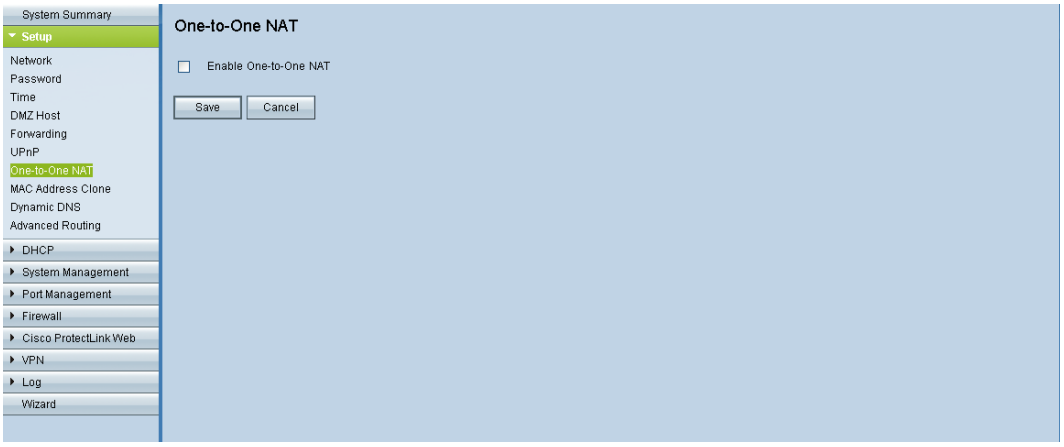
Configuration de la fonctionnalité NAT One-to-One

Utilisez la page *Setup > One-to-One NAT* pour activer la traduction d'adresses réseau NAT (Network Address Translation) One-to-One. Ce processus crée une relation qui associe une adresseIP externe valide à une adresseIP interne masquée par la fonctionnalité NAT. Le trafic peut alors être acheminé depuis Internet vers la ressource interne spécifiée.

REMARQUE Pour obtenir des résultats optimaux, réservez les adressesIP des ressources internes auxquelles vous souhaitez accéder via la fonctionnalité NAT One-to-One. Voir **À propos des adresses IP statiques (pour IPv4 uniquement), page 68**.

Vous pouvez associer une seule relation ou mettre en correspondance une plage d'adressesIP interne avec une plage externe de même longueur (par exemple, trois adresses internes et trois adresses externes). La première adresse interne est associée à la première adresse externe, la deuxième adresseIP interne à la seconde adresse externe et ainsi de suite.

Pour ouvrir cette page : cliquez sur **Setup > One-to-One NAT** dans l'arborescence.



REMARQUE Avant de quitter cette page, cliquez sur **Save** pour enregistrer vos paramètres ou sur **Cancel** pour les annuler. Les modifications non enregistrées ne sont pas prises en compte.

Pour activer cette fonctionnalité, cochez la case **Enable One-to-One NAT**. Ajoutez ou modifiez les entrées, selon vos besoins.

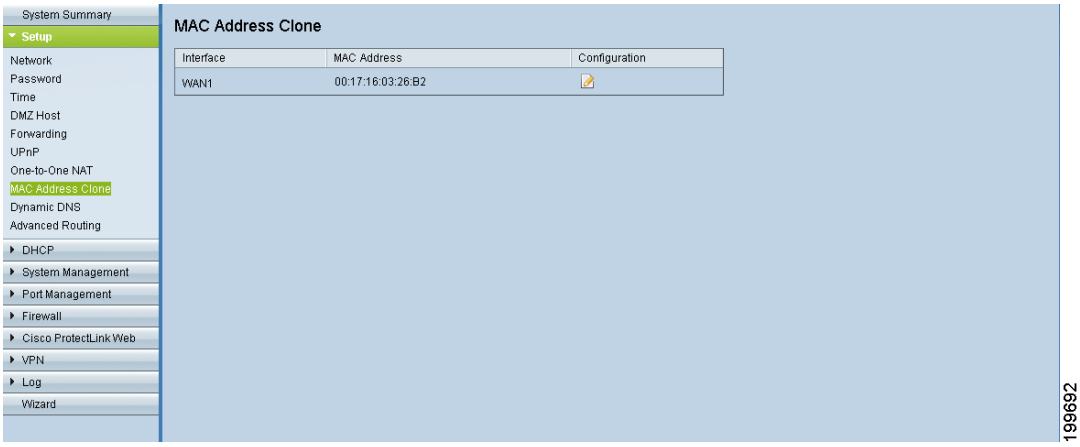
- **Pour ajouter une entrée à la liste:** saisissez les informations suivantes, puis cliquez sur **Add to list**.
  - **Private Range Begin:** saisissez l'adresseIP de départ de la plage d'adressesIP internes que vous souhaitez mettre en correspondance avec la plage publique. N'incluez pas l'adresseIP LAN du routeur dans cette plage.
  - **Public Range Begin:** saisissez l'adresseIP de départ de la plage d'adressesIP publiques spécifiée par le fournisseur d'accès à Internet. N'incluez pas l'adresseIP WAN du routeur dans cette plage.
  - **Range Length:** saisissez le nombre d'adressesIP dans la plage. La longueur de la plage ne doit pas dépasser le nombre d'adressesIP valides. Pour associer une seule adresse, saisissez1.
- **Pour ajouter une nouvelle entrée:** saisissez les informations, puis cliquez sur **Add to list**.
- **Pour modifier une entrée de la liste:** cliquez sur l'entrée à modifier. Les informations apparaissent dans les champs de texte. Apportez les modifications voulues, puis cliquez sur **Update**. Si aucune modification n'est nécessaire, cliquez sur **Add New** pour désélectionner l'entrée et effacer le contenu des champs de texte.

- **Pour supprimer une entrée de la liste:** cliquez sur l'entrée à supprimer, puis sur **Delete**. Pour sélectionner un bloc d'entrées, cliquez sur la première entrée, maintenez la touche **Maj** enfoncée, puis cliquez sur la dernière entrée du bloc. Pour sélectionner des entrées individuellement, maintenez la touche **Ctrl** enfoncée, tout en cliquant sur chacune des entrées en question. Pour annuler la sélection d'une entrée, maintenez la touche **Ctrl** enfoncée tout en cliquant sur l'entrée.

Clonage d'une adresse MAC pour le routeur

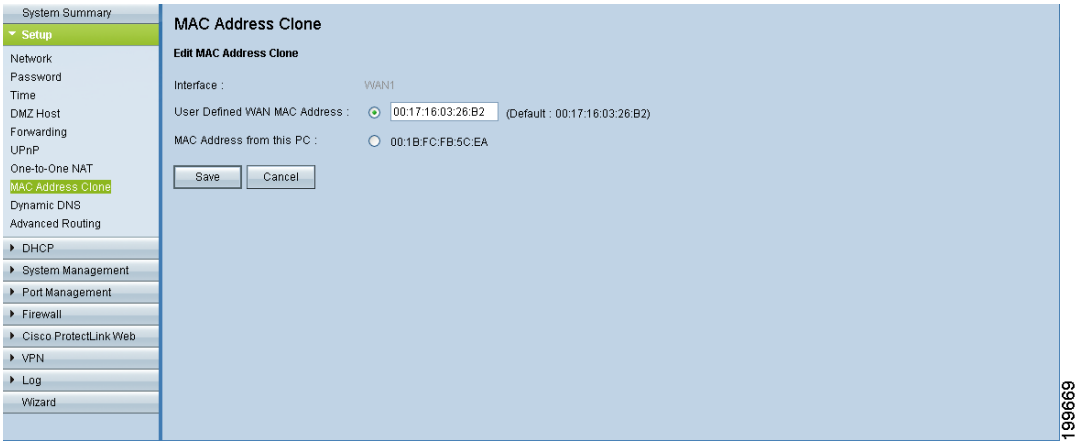
Certains fournisseurs d'accès à Internet exigent que vous enregistriez l'adresse MAC. Cette dernière correspond à un code à 12chiffres attribué à un appareil unique, à des fins d'identification. Si vous avez précédemment enregistré une autre adresse MAC, auprès de votre fournisseur d'accès à Internet, vous pouvez utiliser la page *Setup> MAC Address Clone* afin de «cloner» cette adresse sur votre routeur de la gamme Cisco RV0xx. Grâce à ce processus, vous n'avez pas besoin de contacter votre fournisseur d'accès à Internet pour modifier l'adresse MAC enregistrée.

Pour ouvrir cette page: cliquez sur **Setup> MAC Address Clone** dans l'arborescence.



Cette page affiche les paramètres actuels. Cliquez sur l'icône **Edit** pour afficher la page *Edit MAC Address Clone*. Pour obtenir plus d'informations, reportez-vous à **Modification des paramètres de clonage d'une adresse MAC, page 56**.

Modification des paramètres de clonage d'une adresse MAC



La page *Edit MAC Address Clone* s'affiche dès que vous cliquez sur l'icône **Edit** dans la page *MAC Address Clone*.

REMARQUE Avant de quitter cette page, cliquez sur **Save** pour enregistrer les paramètres ou sur **Cancel** pour les annuler. Les modifications non enregistrées ne sont pas prises en compte.

Pour cloner une adresse MAC, définissez les paramètres suivants.

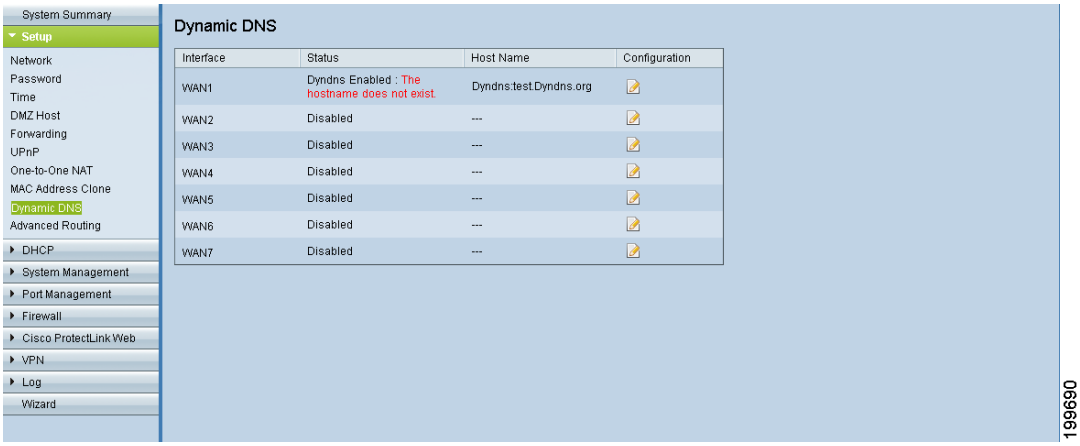
- **User Defined WAN MAC Address :** pour cloner manuellement une adresse MAC, cliquez sur la case d'option, puis saisissez les 12chiffres de l'adresse MAC que vous avez enregistrée auprès de votre fournisseur d'accès à Internet.
- **MAC Address from this PC :** cliquez sur cette case d'option pour cloner l'adresse MAC de l'ordinateur que vous utilisez actuellement pour configurer le routeur. L'adresse MAC de votre PC s'affiche automatiquement.

Attribution d'un nom d'hôte DNS dynamique à une interface WAN

Le service DDNS (Dynamic Domain Name System) vous permet d'attribuer un nom de domaine fixe à une adresse IP WAN dynamique. Vous pouvez ainsi héberger votre propre serveur Web, FTP ou tout autre type de serveur TCP/IP dans votre réseau local. Utilisez la page *Setup> Dynamic DNS* pour configurer les interfaces WAN avec les informations DNS dynamiques en votre possession.

Avant de configurer le service DNS dynamique sur le routeur, visitez le site www.dyndns.org et enregistrez un nom de domaine. Ce service est fourni par DynDNS.org. Pour les utilisateurs résidant en Chine, visitez le site www.3322.org pour procéder à l'enregistrement.

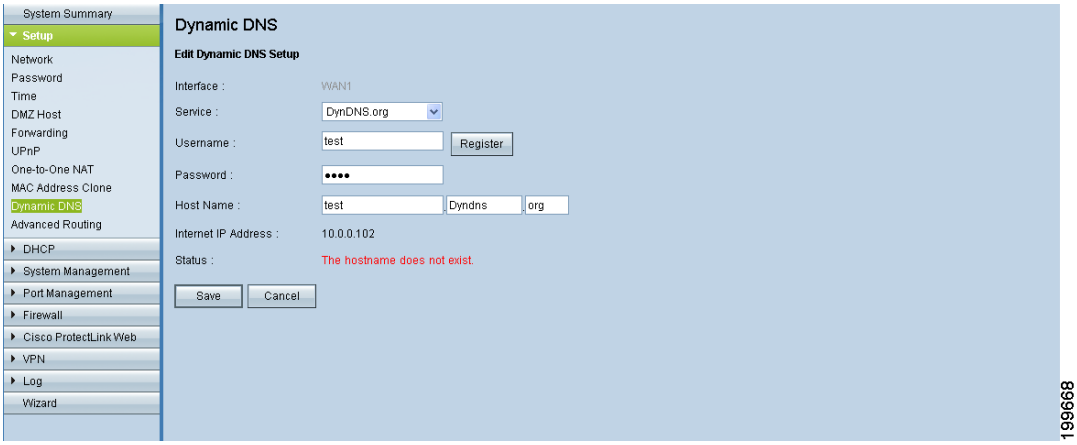
Pour ouvrir cette page: Cliquez sur **Setup> Dynamic DNS** dans l'arborescence.



REMARQUE Avant de quitter cette page, cliquez sur **Save** pour enregistrer vos paramètres ou sur **Cancel** pour les annuler. Les modifications non enregistrées ne sont pas prises en compte.

Cette page affiche les paramètres actuels. Cliquez sur l'icône **Edit** de l'interface WAN pour afficher la page *Edit Dynamic DNS Setup*. Pour obtenir plus d'informations, reportez-vous à la **Modification de la configuration du service Dynamic DNS, page 58**.

Modification de la configuration du service Dynamic DNS



La page *Edit Dynamic DNS Setup* s'affiche lorsque vous cliquez sur une icône **Edit** de la page *Dynamic DNS*.

REMARQUE Avant de quitter cette page, cliquez sur **Save** pour enregistrer les paramètres ou sur **Cancel** pour les annuler. Les modifications non enregistrées ne sont pas prises en compte.

Dans la liste **DDNS Service**, sélectionnez votre service. Saisissez ensuite les informations relatives à votre compte, comme décrit ci-après. Pour désactiver cette option, sélectionnez **Disable**.

- **Username:** saisissez le nom d'utilisateur de votre compte DDNS.

  Si vous n'avez pas encore enregistré de nom d'hôte, vous pouvez cliquer sur **Register** pour accéder au site Web DynDNS.com et vous inscrire gratuitement au service Dynamic DNS. Cliquez sur le lien **Sign up FREE**, puis effectuez toutes les étapes de la procédure.

- **Password:** saisissez le mot de passe de votre compte DDNS.

- **Host Name:** saisissez dans ces trois champs le nom d'hôte que vous avez enregistré auprès de votre fournisseur DDNS. Par exemple, si votre nom d'hôte est *mamaison.dyndns.org*, saisissez *mamaison* dans le premier champ, *dyndns* dans le second et *org* dans le dernier.

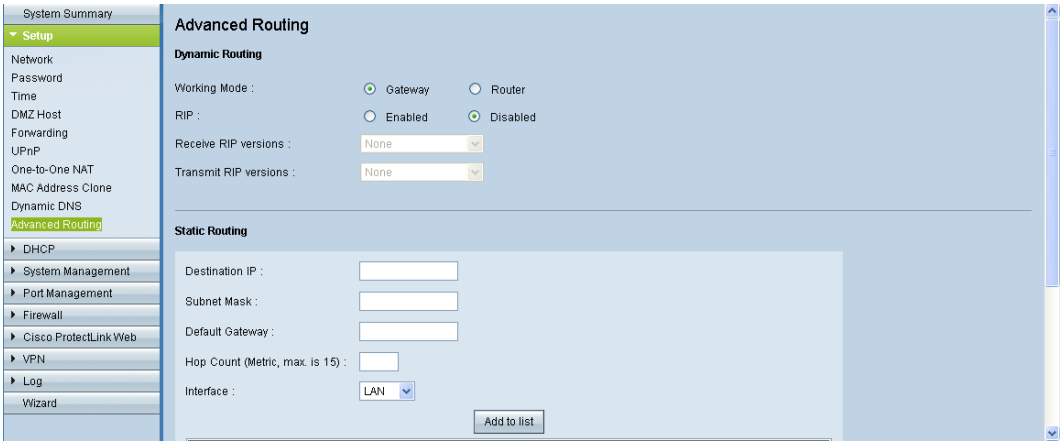
Les informations en lecture seule suivantes s'affichent:

- **Internet IP Address:** adresse IP WAN actuelle de l'interface. Comme cette adresse est dynamique, elle est conçue pour changer.
- **Status:** état de la fonction DDNS. Si les informations sur l'état indiquent une erreur, vérifiez que vous avez correctement saisi les informations relatives à votre compte, pendant la configuration du service DDNS.

Configuration du routage avancé

Utilisez la page *Setup> Advanced Routing* pour configurer les paramètres de routage statique et dynamique et afficher les informations de routage actuelles.

Pour ouvrir cette page: Cliquez sur **Setup> Advanced Routing** dans l'arborescence.



REMARQUE Avant de quitter cette page, cliquez sur **Save** pour enregistrer vos paramètres ou sur **Cancel** pour les annuler. Les modifications non enregistrées ne sont pas prises en compte.

Effectuez les opérations suivantes:

- **Pour configurer le routage statique ou dynamique:** Cliquez sur l'onglet **IPv4** ou **IPv6**, puis définissez les paramètres qui conviennent. Reportez-vous aux sections suivantes:
  - **Configuration du routage dynamique, page 60**
  - **Configuration du routage statique, page 61**
- **Pour afficher les données actuelles:** cliquez sur **View** en bas de la page. La liste *Routing Table Entry List* apparaît. Vous pouvez cliquer sur **Refresh** pour mettre à jour les données ou sur **Close** pour fermer la fenêtre contextuelle.

Configuration du routage dynamique

Configurez les paramètres de **Dynamic Routing** à l'aide du **Routing Information Protocol (RIP)** (voir la définition du Glossaire).

Routage dynamique pour IPv4:

Cliquez sur l'onglet **IPv4**, puis définissez les paramètres décrits ci-après.

- **Working Mode** : sélectionnez l'une des options suivantes:
  - **Gateway :** sélectionnez ce mode si le routeur héberge la connexion de votre réseau à Internet. Il s'agit du paramètre par défaut.
  - **Router :** sélectionnez ce mode si le routeur se trouve sur un réseau comportant d'autres routeurs, et qu'un autre routeur joue le rôle de la passerelle réseau à Internet. En mode Router, la connectivité à Internet n'est disponible que si vous disposez d'un autre routeur jouant le rôle de passerelle. Étant donné que la protection par pare-feu est assurée par le routeur-passerelle, désactivez le pare-feu de ce routeur. Reportez-vous à **Configuration des paramètres de pare-feu généraux, page 102**.
- **RIP :** le protocole RIP (Routing Information Protocol) permet à un routeur d'échanger automatiquement ses informations de routage avec d'autres routeurs et d'adapter ses tables de routage de manière dynamique, en fonction des changements survenant sur le réseau. Le protocole RIP empêche le routage de boucles en fixant un nombre limite d'étapes. Pour activer cette option, sélectionnez **Enabled**. Sinon, conservez le paramètre par défaut, **Disabled**. Si vous activez cette fonctionnalité, configurez également les paramètres suivants:
- **Receive RIP versions :** sélectionnez le protocole RIP permettant de recevoir les données réseau: **None**, **RIPv1**, **RIPv2** ou **Both RIP v1 and v2**.

  RIPv1 est une version de routage à base de classes. Il n'inclut pas d'informations de sous-réseau et ne prend pas en charge, par conséquent, les masques de sous-réseau à longueur variable (VLSM). RIPv1 ne propose pas non plus de prise en charge pour l'authentification du routeur, ce qui le rend vulnérable aux attaques. **RIPv2** dispose d'un masque de sous-réseau et prend en charge la sécurité avec authentification par mot de passe.
- **Transmit RIP versions :** sélectionnez le protocole RIP permettant de transmettre les données réseau: **None**, **RIPv1**, **RIPv2- Broadcast** ou **RIPv2- Multicast**.

RIPv2 - Broadcast (recommandé) diffuse les données dans l'ensemble du sous-réseau. **RIPv2 - Multicast** envoie les données vers des adresses de multidiffusion. RIPv2- Multicast permet également d'éviter toute charge inutile en diffusant des tables de routage à des routeurs adjacents au lieu de les transmettre à l'ensemble du réseau.

Routage dynamique pour IPv6:

REMARQUE L'onglet IPv6 n'est disponible que si vous avez activé l'adresse IP Dual-Stack dans la page *Setup> Network*.

Cochez ou décochez cette case pour activer ou désactiver la fonction **RIPng (RIP next generation)** (voir la définition du Glossaire).

Configuration du routage statique

Configurez les paramètres de **Routage statique** (voir la définition du Glossaire).

AVERTISSEMENT Le routage statique est une fonctionnalité avancée. Apportez le plus grand soin à la création de ces itinéraires.

Ajoutez ou modifiez les entrées, selon vos besoins. N'oubliez pas que les paramètres ne sont pas enregistrés tant que vous n'avez pas cliqué sur le bouton Save.

- **Pour ajouter un itinéraire statique:** saisissez les informations suivantes, puis cliquez sur **Add to list**. Vous pouvez spécifier jusqu'à 30itinéraires.
  - **Destination IP :** saisissez l'adresse réseau du segment LAN distant. Pour un domaineIP de classeC classique, l'adresse réseau se compose des trois premiers champs de l'adresseIP LAN de destination, le dernier champ devant contenir le chiffre zéro.
  - **Subnet Mask (IPv4 uniquement) :** saisissez le masque de sous-réseau utilisé dans le domaineIP LAN de destination. Pour les domaines IP de classeC, le masque de sous-réseau est 255.255.255.0.
  - **Prefix Length (IPv6 uniquement) :** saisissez la longueur de préfixe.
  - **Default Gateway :** saisissez l'adresseIP du routeur du réseau pour lequel cet itinéraire statique est créé. Par exemple, si ce réseau est connecté au port LAN du routeur local via un autre routeur, utilisez l'adresseIP WAN de ce dernier.

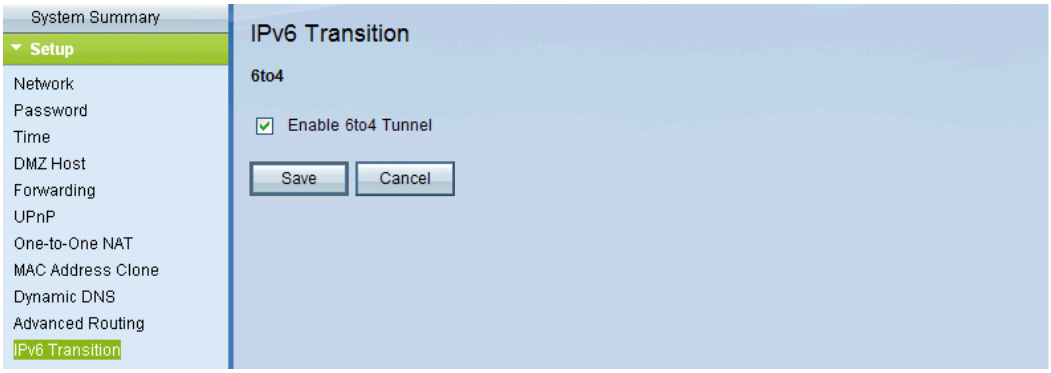
- **Hop Count :** saisissez la valeur appropriée (la valeur maximale est de15). Cette valeur indique le nombre de nœuds que traverse un paquet de données avant d'atteindre sa destination. Un nœud désigne un périphérique du réseau tel qu'un ordinateur ou un routeur.
- **Interface :** sélectionnez l'interface à utiliser pour cet itinéraire. Sélectionnez une interface WAN si ce routeur fournit une connectivité Internet à votre réseau. Sélectionnez **LAN** si ce routeur obtient une connectivité Internet à partir d'un routeur-passerelle sur votre réseau local.

- **Pour ajouter un nouvel itinéraire statique:** saisissez les informations, puis cliquez sur **Add to list**.
- **Pour modifier un itinéraire statique de la liste:** cliquez sur l'entrée à modifier. Les informations apparaissent dans les champs de texte. Apportez les modifications voulues, puis cliquez sur **Update**. Si aucune modification n'est nécessaire, cliquez sur **Add New** pour désélectionner l'entrée et effacer le contenu des champs de texte.
- **Pour supprimer une entrée de la liste:** cliquez sur l'entrée à supprimer, puis sur **Delete**. Pour sélectionner un bloc d'entrées, cliquez sur la première entrée, maintenez la touche **Maj** enfoncée, puis cliquez sur la dernière entrée du bloc. Pour sélectionner des entrées individuellement, maintenez la touche **Ctrl** enfoncée, tout en cliquant sur chacune des entrées en question. Pour annuler la sélection d'une entrée, maintenez la touche **Ctrl** enfoncée tout en cliquant sur l'entrée.
- **Pour afficher les données actuelles:** cliquez sur **View** en bas de la page. La liste *Routing Table Entry List* apparaît. Vous pouvez cliquer sur **Refresh** pour mettre à jour les données ou sur **Close** pour fermer la fenêtre contextuelle.

Transition IPv6

Si l'option Dual-Stack IP est activée dans la page *Network> Setup*, un tunnel 6to4 est activé par défaut pour les paquets IPv6 grâce à l'échange d'adressage source/destination6to4. Cette fonction permet au routeur d'établir un tunnel automatique au niveau du réseauIPv4 (ou une connexion InternetIPv4 réelle) entre deux réseaux IPv6 indépendants. Utilisez la page *Setup> IPv6 Transition* pour activer ou désactiver cette fonction.

Pour ouvrir cette page: cliquez sur **Setup> IPv6 Transition** dans l'arborescence.



Cochez ou décochez cette case pour activer ou désactiver le tunnel 6to4.

REMARQUE Avant de quitter cette page, cliquez sur **Save** pour enregistrer vos paramètres ou sur **Cancel** pour les annuler. Les modifications non enregistrées ne sont pas prises en compte.

Étapes suivantes: lors d'un déploiement classique (configuration d'un tunnel 6to4 entre votre routeur RV0xx et un routeur CiscoRV sur un autre site), il est nécessaire d'effectuer les opérations décrites ci-après.

- Sur la page *DHCP->Router Advertisement*, activez les indicateurs RA gérés pour prendre en charge la configuration automatique des périphériques connectés. Assurez-vous que vos périphériques IPv6 disposent des préfixes 6to4. Les préfixes se présentent sous la forme suivante: 2002:*<votre adresse IP WAN au format hexadécimal>*::)
- Désactivez temporairement le pare-feu du routeur afin de tester votre tunnel 6to4. À la page *Firewall> General* page, choisissez **Disable**. Pour tester le tunnel, essayez d'effectuer un ping sur l'adresse IPv6 au niveau du site distant.

- Après avoir vérifié le tunnel comme indiqué ci-avant, activez le pare-feu et ajoutez des règles d'accès sur la page *Firewall >Access Rules*. Ajoutez, par exemple, une règle pour autoriser tout le trafic transitant par l'interface WAN dans les conditions suivantes: la source correspond à une adresseIP unique ou à une plage d'adresses sur le réseau local et la destination correspond à une adresseIP unique ou à une plage d'adresses sur le réseau distant.
- Effectuez les opérations requises sur le routeur à l'autre extrémité du tunnel 6to4.

REMARQUE Pour plus d'informations à ce sujet, reportez-vous aux liens vers la documentation indiqués à l'**Annexe H, « Pour en savoir plus »**..

4

DHCP

Le module *DHCP* sert à configurer les paramètres du serveur DHCP ou de l'agent de relais DHCP, ainsi qu'à afficher le récapitulatif des informations sur DHCP.

Si l'adresse IP Dual-Stack est activée dans la page *Network > Setup*, vous pouvez configurer les paramètres IPv4 et IPv6.

Reportez-vous aux rubriques suivantes:

Configuration du serveur DHCP ou du relais DHCP

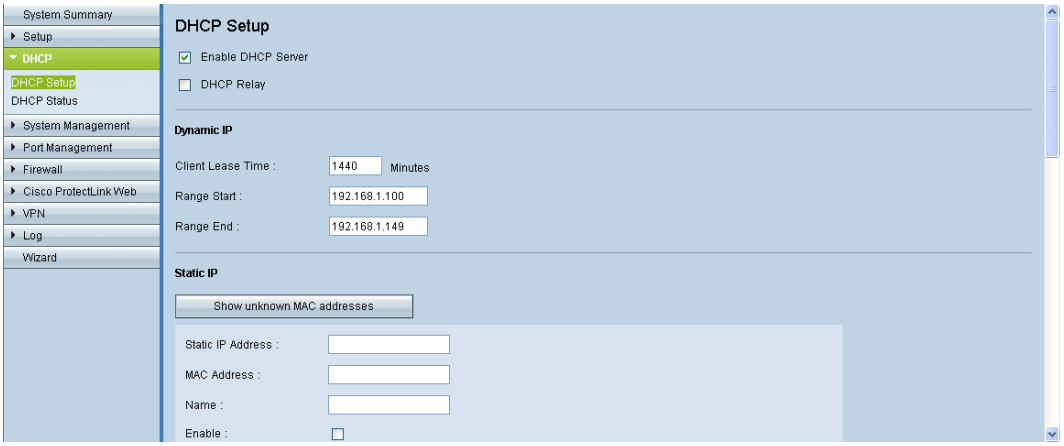
Utilisez la page *DHCP > DHCP Setup* pour configurer ce routeur en tant que serveur DHCP (Dynamic Host Configuration Protocol) ou en tant qu'agent de relais DHCP.

Le serveur DHCP attribue automatiquement les adresses IP disponibles aux ordinateurs de votre réseau. Une adresse est «louée» à un client donné pendant une durée spécifiée, puis elle arrive à expiration et peut être attribuée à un autre périphérique. Pour attribuer une adresse permanente à un périphérique, vous pouvez ajouter le périphérique à la liste des adresses IP statiques. Vous pouvez également utiliser la liste d'adresses IP statiques pour bloquer l'accès des périphériques qui ne figurent pas sur la liste ou qui ne sont pas dotés de l'adresse IP correcte.

Si votre réseau comprend un autre serveur DHCP ou que vous souhaitez attribuer des adresses IP manuellement, vous pouvez désactiver la fonctionnalité DHCP et activer le relais DHCP. Pour obtenir plus d'informations, reportez-vous à la section **Activation d'un serveur DHCP et d'un relais DHCP, page 66**.

REMARQUE Le relais DHCP n'est disponible que sous l'onglet IPv4. Le relais DHCPv6 n'est pas disponible.

Pour ouvrir cette page : Cliquez sur **DHCP > DHCP Setup** dans l'arborescence.



REMARQUE Avant de quitter cette page, cliquez sur **Save** pour enregistrer vos paramètres ou sur **Cancel**, pour les annuler. Les modifications non enregistrées ne sont pas prises en compte.

Activation d'un serveur DHCP et d'un relais DHCP

Cliquez sur l'onglet **IPv4** ou l'onglet **IPv6**.
Remarque: L'onglet IPv6 n'est disponible que si vous avez activé l'adresse IP Dual-Stack dans la page *Network > Setup*.

Saisissez les paramètres suivants :

- **Enable DHCP Server:** cochez la case pour permettre au routeur d'attribuer de manière dynamique les adresses IP jusqu'à 50 périphériques reliés. Décochez la case si vous avez un autre serveur DHCP sur le réseau ou si vous voulez configurer les adresses IP statiques pour vos périphériques réseau. Si vous avez activé cette fonction, entrez les paramètres dans la section **Dynamic IP** de la page comme décrit ci-dessous. Les autres sections de cette page sont facultatives.
- **DHCP Relay (IPv4 uniquement):** si vous disposez d'un autre serveur DHCP, activez le relais DHCP pour permettre à ce routeur de communiquer les requêtes DHCP des clients au serveur DHCP. Grâce au mécanisme de relais DHCP, les clients DHCP et le serveur DHCP peuvent résider sur des réseaux distincts. Les clients DHCP envoient des paquets d'émission de découverte DHCP pour obtenir les adresses IP du serveur DHCP. Ce routeur agit en tant qu'agent de relais DHCP et envoie des réponses de monodiffusion DHCP au serveur DHCP.

Obligatoire : saisissez l'**adresse IP du serveur DHCP**. Les autres sections de cette page sont facultatives.

REMARQUE *IPv4 uniquement:* si vous désactivez le serveur DHCP et le relais DHCP, configurez chaque périphérique de votre réseau avec une adresse IP statique, un masque de sous-réseau et des paramètres DNS. N'attribuez pas la même adresse IP à plusieurs ordinateurs.

Adresse IP dynamique (utilisée uniquement pour le serveur DHCP)

- **Client Lease Time:** la durée de bail du client est la durée pendant laquelle l'utilisateur d'un réseau est autorisé à se connecter au routeur à l'aide de l'adresse IP dynamique actuelle. Saisissez la durée, en minutes. Les valeurs valides sont comprises entre 5 et 43 200 minutes. La valeur par défaut est 1440 minutes, soit 24heures.

  REMARQUE: pour pouvoir recevoir une adresse IP du serveur DHCP, le périphérique client doit être configuré pour pouvoir obtenir une adresse IP automatiquement d'un serveur DHCP. Par défaut, les ordinateurs Windows sont configurés pour obtenir une adresse IP automatiquement.

- **Range Start** et **Range End:** saisissez une adresse IP de début et une adresse IP de fin pour créer une plage d'adresses IP pouvant être attribuées de manière dynamique. La plage peut comprendre jusqu'à 50 adresses IP, nombre maximum d'adresses IP pouvant être attribuées par le serveur. Les valeurs valides sont comprises entre 100 et 149. N'incluez pas l'adresseIP LAN du routeur dans cette plage d'adresses IP dynamiques. Par exemple, si le routeur utilise l'adresse IP LAN par défaut (**192.168.1.1**), la valeur de début doit être 192.168.1.2 ou plus.

DNS (utilisé uniquement pour le serveur DHCP)

Vous pouvez saisir l'adresse IP d'un **serveur DNS**. Vous pouvez aussi saisir un serveur DNS secondaire. La saisie d'un serveur DNS peut permettre un accès plus rapide que l'utilisation d'un serveur DNS attribué de manière dynamique par le biais des paramètres WAN. Vous pouvez conserver le paramètre par défaut (0.0.0.0) pour utiliser un serveur DNS attribué de manière dynamique.

WINS (utilisé uniquement pour le serveur DHCP, IPv4)

Vous pouvez également saisir l'adresse IP d'un **serveur WINS**. Le service WINS (Windows Internet Naming Service) résout les noms NetBIOS en adresses IP. Si vous ne connaissez pas l'adresse IP du serveur WINS, conservez la valeur par défaut, 0.0.0.0.

REMARQUE Pour prendre en charge NetBIOS pour les clients DHCP, le routeur utilise deux méthodes différentes:

- Lorsqu'un client DHCP reçoit des adresses IP dynamiques du routeur, il inclut automatiquement les informations du serveur WINS, afin de pouvoir prendre en charge NetBIOS.
- Si un client est doté d'une adresse IP statique, l'adresse IP, le masque de sous-réseau, l'adresse de la passerelle par défaut et les paramètres du serveur DNS doivent être configurés à la page Protocole Internet (TCP/IP) du système d'exploitation Windows. L'adresse IP WINS doit ensuite être configurée à la page Paramètres TCP/IP avancés. (Pour obtenir plus d'informations, reportez-vous à l'aide de Windows.)

À propos des adresses IP statiques (pour IPv4 uniquement)

Lorsque DHCP est activé, vous pouvez attribuer des adresses IP statiques à certains périphériques tels que les serveurs Web ou les serveurs FTP. Vous pouvez ajouter jusqu'à 100 périphériques à la liste *Static IP*.

CONSEIL Vérifiez que chacun de ces périphériques est configuré pour utiliser une adresse IP statique. Par exemple, sur un ordinateur Windows, ouvrez les Propriétés de la connexion au réseau local, sélectionnez **Protocole Internet (TCP/IP)** puis cliquez sur le bouton **Propriétés**. Choisissez **Utiliser l'adresse IP suivante**, puis saisissez l'adresse IP, le masque de sous-réseau et la passerelle par défaut (l'adresse IP du routeur). Vous pouvez, en option, saisir le serveur DNS qui a votre préférence.

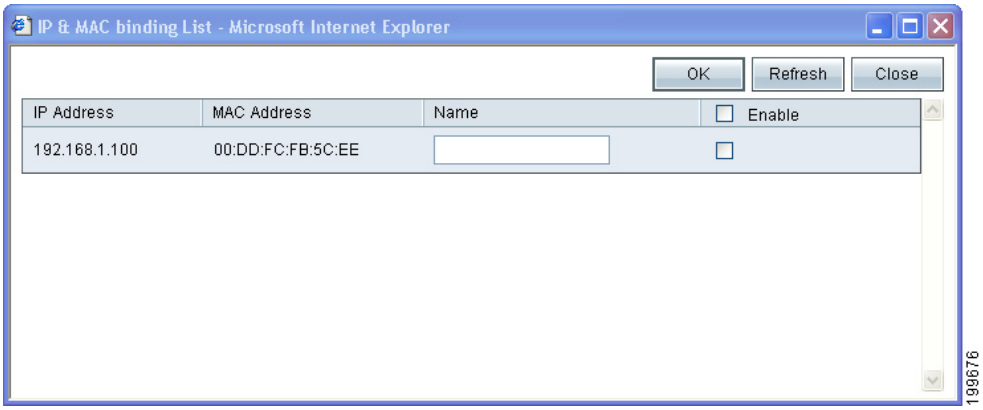
Choisissez les périphériques dans une liste ou saisissez manuellement les adresses IP et les adresses MAC des périphériques.

- **Attribuer des adresses IP statiques en ajoutant des périphériques à partir d'une liste, page 69**
- **Attribuer des adresses IP statiques en saisissant manuellement des périphériques, page 70**
- **Utilisation de la liste d'adresses IP statiques pour bloquer des périphériques, page 71**

REMARQUE Vous pouvez utiliser cette fonctionnalité même si le routeur n'est pas un serveur DHCP.

Attribuer des adresses IP statiques en ajoutant des périphériques à partir d'une liste

STEP 1 Cliquez sur **Show unknown MAC addresses**. La liste *IP & MAC binding list* s'affiche. Si le navigateur Web affiche un message relatif à la fenêtre contextuelle, autorisez le contenu bloqué.



Les périphériques sont répertoriés en fonction de leurs adresses IP et MAC. (L'adresse MAC est généralement indiquée sur une étiquette située au-dessous ou au dos du périphérique.) Au besoin, vous pouvez cliquer sur **Refresh** pour mettre à jour les données.

STEP 2 Pour sélectionner un périphérique, saisissez d'abord un **nom** descriptif. Activez ensuite la case **Enable**. Vous pouvez également sélectionner tous les périphériques de la liste en cliquant sur la case à cocher située en haut de la colonne *Enable*.

STEP 3 Cliquez sur **OK** pour ajouter les périphériques à la liste *Static IP* ou cliquez sur **Close**, pour fermer la fenêtre contextuelle sans ajouter les périphériques sélectionnés. Une fois que vous avez cliqué sur **OK**, un message apparaît. Le message comprend d'importantes informations. Lisez-le, puis cliquez sur **OK**. Laissez le navigateur ouvert et attendez que les adresses MAC sélectionnées apparaissent dans la liste *Static IP*.

STEP 4 Modifiez ou supprimez des entrées de la liste, si nécessaire.

- **Pour modifier les paramètres :** cliquez dans un périphérique de la liste. Les informations relatives à cet utilisateur apparaissent dans les champs textuels. Modifiez à votre guise, puis cliquez sur **Update**. Si aucune modification n'est nécessaire, cliquez sur **Add New,** pour désélectionner l'entrée et faire disparaître les champs textuels.

- **Pour supprimer une entrée de la liste :** cliquez sur l'entrée à supprimer, puis sur **Delete**. Pour sélectionner un bloc d'entrées, cliquez sur la première entrée, maintenez la touche **Maj** enfoncée, puis cliquez sur la dernière entrée du bloc. Pour sélectionner des entrées individuellement, maintenez la touche **Ctrl** enfoncée, tout en cliquant sur chacune des entrées en question. Pour annuler la sélection d'une entrée, maintenez la touche **Ctrl** enfoncée, tout en cliquant sur l'entrée.

Attribuer des adresses IP statiques en saisissant manuellement des périphériques

Dans la section *Static IP Address*, ajoutez ou modifiez des entrées, si nécessaire. N'oubliez pas que les paramètres ne sont pas enregistrés tant que vous n'avez pas cliqué sur le bouton Save.

- **Pour ajouter un nouveau périphérique à la liste:** saisissez les informations suivantes, puis cliquez sur **Add to list**.
  - **Static IP Address :** saisissez l'adresse IP statique. Saisissez 0.0.0.0 si vous voulez que le routeur attribue une adresse IP statique au périphérique.
  - **MAC Address :** saisissez l'adresse MAC du périphérique. (L'adresse MAC est généralement indiquée sur une étiquette située au-dessous ou au dos du périphérique.) Saisissez l'adresse sans marque de ponctuation.
  - **Name:** saisissez un nom descriptif pour le périphérique.
  - **Enable:** cochez cette case pour attribuer l'adresse IP statique à ce périphérique.
- **Pour ajouter une nouvelle entrée :** saisissez les informations, puis cliquez sur **Add to list**.
- **Pour modifier les paramètres :** cliquez dans un périphérique de la liste. Les informations relatives à cet utilisateur apparaissent dans les champs textuels. Modifiez à votre guise, puis cliquez sur **Update**. Si aucune modification n'est nécessaire, cliquez sur **Add New,** pour désélectionner l'entrée et faire disparaître les champs textuels.
- **Pour supprimer une entrée de la liste :** cliquez sur l'entrée à supprimer, puis sur **Delete**. Pour sélectionner un bloc d'entrées, cliquez sur la première entrée, maintenez la touche **Maj** enfoncée, puis cliquez sur la dernière entrée du bloc. Pour sélectionner des entrées individuellement, maintenez

la touche **Ctrl** enfoncée, tout en cliquant sur chacune des entrées en question. Pour annuler la sélection d'une entrée, maintenez la touche **Ctrl** enfoncée, tout en cliquant sur l'entrée.

Utilisation de la liste d'adresses IP statiques pour bloquer des périphériques

Vous pouvez utiliser la *liste d'adresses IP statiques* pour contrôler l'accès à votre réseau. Vous pouvez interdire l'accès aux périphériques qui ne figurent pas sur la liste ou qui ne possèdent pas l'adresse IP correcte.

STEP 1 Pour ajouter des périphériques à la *liste d'adresses IP statiques*, reportez-vous à la section**À propos des adresses IP statiques (pour IPv4 uniquement), page 68**.

STEP 2 Activez ou désactivez les fonctionnalités suivantes:

- **Block MAC address on the list with wrong IP address :** cochez cette case pour empêcher un ordinateur d'accéder à votre réseau si son adresse IP a été modifiée. Par exemple, si vous aviez précédemment attribué l'adresse IP statique 192.168.1.100 à l'ordinateur et qu'une autre personne configure l'ordinateur pour utiliser l'adresse 192.168.149, le périphérique n'est pas autorisé à se connecter à votre réseau. Cette fonctionnalité permet de dissuader les utilisateurs de changer les adresses IP de leur ordinateur sans votre autorisation. Désactivez la case pour autoriser l'accès quelle que soit l'adresse IP actuellement attribuée.
- **Block MAC address not on the list :** cochez cette case pour interdire l'accès aux périphériques qui ne figurent pas dans la *liste d'adresses IP statiques*. Cette fonctionnalité permet d'empêcher que des périphériques inconnus accèdent à votre réseau. Désactivez la case pour autoriser l'accès à n'importe quel périphérique connecté configuré avec une adresse IP comprise dans la plage correcte.

Base de données DNS locale

Le service DNS (Domain Name Service, service de noms de domaine) est un service qui fait correspondre les noms de domaine à des adresses IP routables. Vous pouvez configurer une base de données DNS locale qui permette au routeur d'agir en tant que serveur DNS local pour les noms de domaine couramment utilisés. L'utilisation d'une base de données locale peut s'avérer plus rapide que celle d'un serveur DNS externe. Si un nom de domaine demandé n'est pas trouvé dans la base de données locale, la requête est transmise au serveur DNS spécifié à la page *Setup > Network* , dans la section *WAN Setting*.

Si vous activez cette fonctionnalité, vous devez également configurer les périphériques clients pour utiliser le routeur en tant que serveur DNS. Par défaut, les ordinateurs Windows sont configurés pour obtenir une adresse de serveur DNS automatiquement, à partir des paramètres WAN. Vous devez changer les paramètres de connexion TCP/IP. Par exemple, sur un ordinateur Windows, ouvrez la boîte de dialogue *Propriétés de la connexion au réseau local > Protocole Internet > TCP/IP Properties*. Choisissez *Utiliser l'adresse de serveur DNS suivante*, puis saisissez l'adresse IP LAN du routeur comme serveur DNS préféré. Pour obtenir plus d'informations, reportez-vous à la documentation du client que vous configurez.

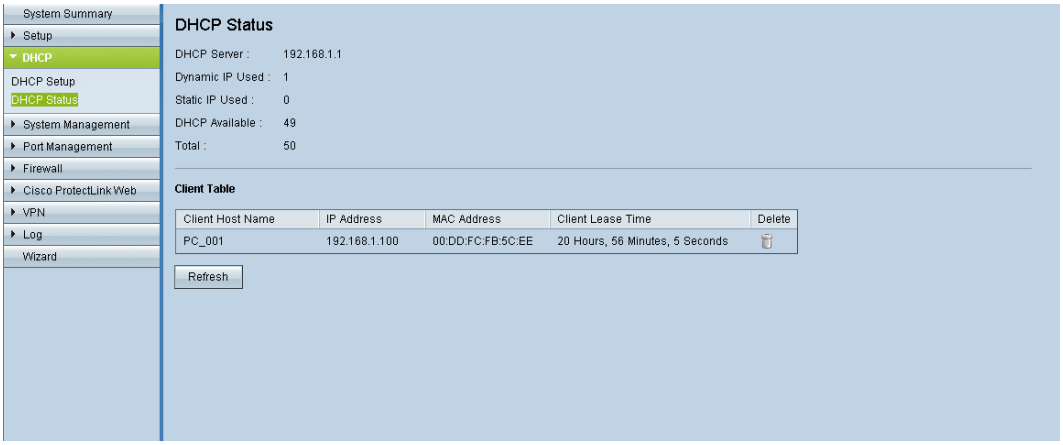
Ajoutez ou mettez à jour les entrées, selon les besoins. N'oubliez pas que les paramètres ne sont pas enregistrés tant que vous n'avez pas cliqué sur le bouton Save.

- **Pour ajouter une nouvelle entrée :** Saisissez les informations suivantes. Puis cliquez sur **Add to list**.
  - **Host Name:** saisissez le nom de domaine, tel que *exemple.com* ou *exemple.org*. Si vous n'incluez pas la fin du nom de domaine, Microsoft Windows® ajoute automatiquement *.com* à la fin de votre saisie.
  - **IP Address**: entrez l'adresse IP de la ressource.
- **Pour ajouter une nouvelle entrée :** saisissez les informations, puis cliquez sur **Add to list**.
- **Pour modifier les paramètres d'un périphérique :** cliquez dans un périphérique de la liste. Les informations relatives à cet utilisateur apparaissent dans les champs textuels. Modifiez à votre guise, puis cliquez sur **Update**. Si aucune modification n'est nécessaire, cliquez sur **Add New,** pour désélectionner l'entrée et faire disparaître les champs textuels.
- **Pour supprimer une entrée de la liste :** cliquez sur l'entrée à supprimer, puis sur **Delete**. Pour sélectionner un bloc d'entrées, cliquez sur la première entrée, maintenez la touche **Maj** enfoncée, puis cliquez sur la dernière entrée du bloc. Pour sélectionner des entrées individuellement, maintenez la touche **Ctrl** enfoncée, tout en cliquant sur chacune des entrées en question. Pour annuler la sélection d'une entrée, maintenez la touche **Ctrl** enfoncée, tout en cliquant sur l'entrée.

Affichage des informations sur l'état du serveur DHCP

Utilisez la page *DHCP > Status* pour visualiser l'état du serveur DHCP et de ses clients. Vous pouvez cliquer sur **Refresh** pour actualiser les données. Pour libérer l'adresse IP d'un client, vous pouvez cliquer sur l'icône **Supprimer**.

Pour ouvrir cette page : Cliquez sur **DHCP > DHCP Status** dans l'arborescence.



Serveur DHCP

Pour le serveur DHCP, les informations suivantes sont affichées:

- **DHCP Server:** adresse IP pour le serveur DHCP.
- **Dynamic IP Used :** nombre d'adresses IP dynamiques utilisées.
- **Static IP Used (IPv4 uniquement) :** nombre d'adresses IP statiques utilisées.
- **DHCP Available :** nombre d'adresses IP dynamiques disponibles.
- **Total:** nombre total d'adresses IP dynamiques pouvant être attribuées par le serveur DHCP.

Client Table

Pour tous les clients du réseau qui utilisent le serveur DHCP, le tableau sur le client comprend des informations sur le client DHCP actuel. Cliquez sur l'onglet **IPv4** ou l'onglet **IPv6** pour afficher les clients.
Remarque: L'onglet IPv6 n'est disponible que si vous avez activé l'adresse IP Dual-Stack dans la page *Network > Setup*.

- **Client Host Name:** nom attribué à un hôte client.

- **IP Address :** adresse IP dynamique attribuée au client.
- **MAC Address (IPv4 uniquement) :** adresse MAC d'un client.
- **Client Lease Time :** durée pendant laquelle l'utilisateur d'un réseau est autorisé à se connecter au routeur à l'aide d'une adresse IP dynamique.
- **Delete (IPv4 uniquement) :** cliquez sur l'icône pour supprimer le bail et déconnecter le client.

Router Advertisement (IPv6)

Utilisez la page *DHCP > Router Advertisement* pour activer le **RADVD (Démon de notification de routeur)** en vue de la configuration automatique des adressesIP des hôtes IPv6 et de leur routage. Lorsque cette fonction est activée, les messages sont envoyés régulièrement au routeur en réponse aux sollicitations. Un hôte utilise les informations pour connaître les préfixes et les paramètres du réseau local. Désactiver cette fonction a pour effet de désactiver la configuration automatique, ce qui nécessite une configuration manuelle de l'adresse IPv6, du préfixe de sous-réseau et de la passerelle par défaut sur chaque périphérique.

Cette page est disponible si vous avez activé l'adresse Dual-Stack dans la page *Setup > Network*. Si tel n'est pas le cas, un message s'affiche lorsque vous tentez d'accéder à cette page. Après avoir lu le message, cliquez sur **OK** pour configurer les paramètres réseau ou simplement sur **Cancel** pour fermer la fenêtre du message.

Pour ouvrir cette page : Cliquez sur **DHCP** > **Router Advertisement** dans l'arborescence.

REMARQUE Avant de quitter cette page, cliquez sur **Save** pour enregistrer vos paramètres ou sur **Cancel**, pour les annuler. Les modifications non enregistrées ne sont pas prises en compte.

- **Enable Router Advertisement :** pour activer la fonction, cochez la case, puis renseignez les autres champs de la page. Pour désactiver la fonction, désactivez la case.
- **Advertise Mode :** sélectionnez l'une des options suivantes:
  - **Unsolicited Multicast :** sélectionnez cette option pour envoyer des messages de notification de routeur à toutes les interfaces du groupe de multidestination. Il s'agit de l'option par défaut. Si vous choisissez cette option, saisissez l'intervalle **Advertisement Interval** qui indique à

quelle fréquence les messages sont envoyés. Saisissez une valeur comprise entre 10 et 1 800 secondes. La valeur par défaut est 30secondes.

- **Unicast only :** sélectionnez cette option pour envoyer des messages de notification de routeur aux adresses IPv6 bien connues.

- **RA Flags :** indiquez si les hôtes peuvent utiliser DHCPv6 pour obtenir les adresses et d'autres informations. Les options sont décrites ci-dessous.
  - *Activation de l'indicateur Managed uniquement:* cochez la case **Managed** si vous voulez que les hôtes utilisent un protocole de configuration administré/dynamique (DHCPv6) pour obtenir les adresses dynamiques et d'autres informations via DHCPv6.
  - *Activation de l'indicateur Other uniquement:* cochez la case **Other** si vous voulez que les hôtes utilisent un protocole de configuration administré/dynamique (DHCPv6) pour obtenir des informations autres que les informations d'adresse, telles que les adresses du serveur DNS.
  - *Activation des deux indicateurs:* cochez les deux cases si vous voulez que les hôtes obtiennent des adresses et d'autres informations via DHCPv6.
  - *Désactivation des deux indicateurs:* désélectionnez les deux cases si vous voulez que les hôtes obtiennent des adresses et d'autres informations via l'annonce de routeur et non par DHCPv6.

- **Router Preference :** Choisissez **High, Medium** ou **Low**. Cette préférence est utile dans le cadre d'une topologie réseau où des hôtes multiréseau ont accès à plusieurs routeurs. La valeur définit aide les hôtes à choisir le routeur approprié. Si deux routeurs sont accessibles, celui qui a la préférence la plus élevée sera choisi. Ces valeurs sont ignorées par les hôtes qui ne prennent pas en charge la préférence du routeur. La valeur par défaut est High.

- **MTU :** saisissez la taille du paquet le plus volumineux pouvant transiter par le réseau. L'unité **Taille maximum de l'unité de transfert (MTU)** permet aux messages de notification de routeur de s'assurer que tous les nœuds du réseau utilisent la même valeur MTU lorsque celle du réseau locale n'est pas connue. La valeur par défaut est 1 500 octets qui correspond à la valeur standard des réseaux Ethernet. Pour les connexions PPPoE, la valeur standard est 1 492 octets. Il est conseillé de ne pas modifier ce paramètre, sauf si votre fournisseur d'accès réseau en requiert un différent.

- **Router Lifetime :** saisissez le nombre de secondes pendant lequel les messages de notification de routeur figurent sur le routage. La valeur par défaut est 3600secondes.

5

Gestion du système

Utilisez le module System Management pour gérer les paramètres avancés, configurer les outils de diagnostic et effectuer des tâches telles que les mises à niveau de microprogramme, les sauvegardes et les redémarrages. Reportez-vous aux rubriques suivantes:

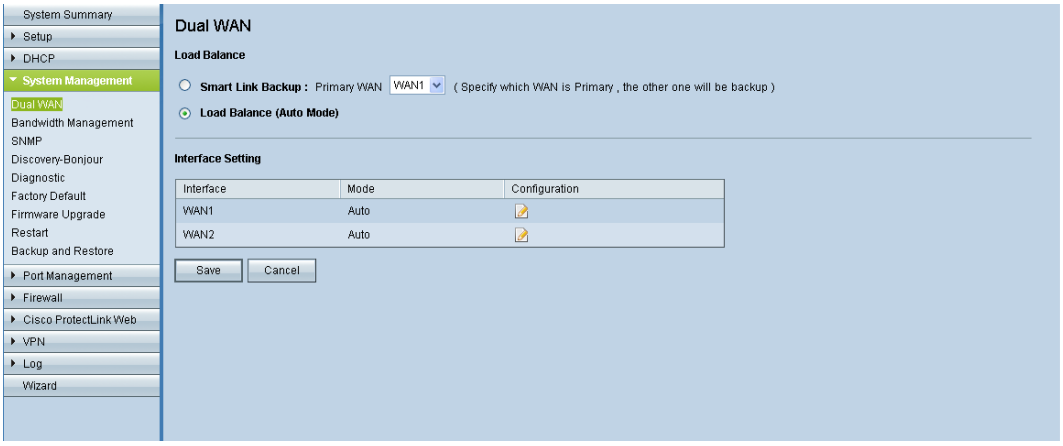
Configuration des connexions WAN et Multi-WAN

Utilisez la page *System Management > Dual WAN* (ou *Multi-WAN* sur le routeur RV016) pour configurer les paramètres de vos connexions Internet, si vous utilisez plusieurs interfaces WAN.

Pour ouvrir cette page: cliquez sur **System Management > Dual WAN (ou Multi-WAN sur le routeur RV016)** dans l'arborescence de navigation.

REMARQUE Avant de quitter cette page, cliquez sur **Save** pour enregistrer vos paramètres ou sur **Cancel** pour les annuler. Les modifications non enregistrées ne sont pas prises en compte.

Mode: Cisco RV042, RV042G et RV082

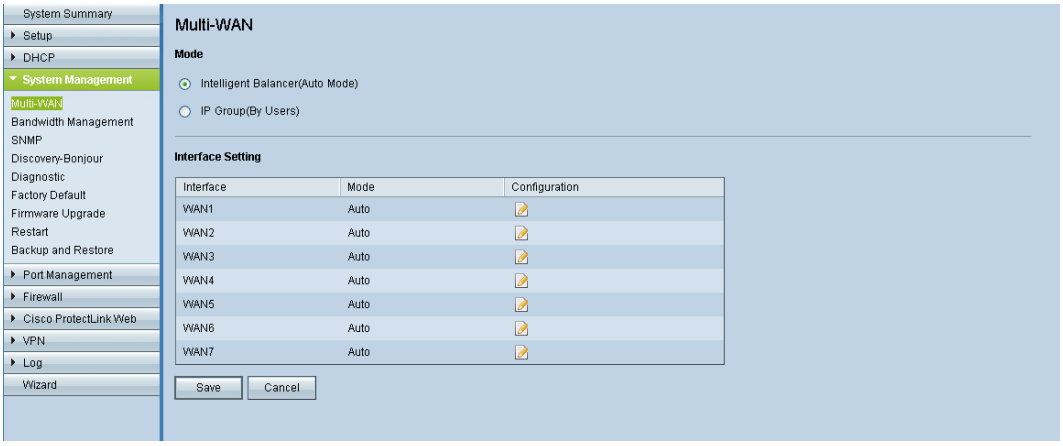


Vous pouvez configurer jusqu'à deux connexions Internet à l'aide du port Internet et du port DMZ/Internet. Vous pouvez choisir l'un des modes suivants pour gérer vos connexions WAN:

- **Smart Link Backup:** choisissez ce mode pour avoir l'assurance d'une connectivité continue. Si la connexion WAN principale n'est pas disponible, la connexion WAN de secours est utilisée.
- **Load Balance:** choisissez ce mode pour utiliser les deux connexions Internet simultanément afin d'augmenter la bande passante disponible. Le routeur équilibre le trafic entre les deux interfaces, par permutation pondérée.

  REMARQUE: les requêtes DNS ne sont pas soumises à l'équilibrage de charge.

Mode: Cisco RV016



Vous pouvez configurer jusqu'à sept connexions Internet en utilisant les deux ports Internet et les cinq ports à double fonction. Vous pouvez choisir l'un des modes suivants pour gérer vos connexions WAN:

- **Intelligent Balancer (Auto Mode):** sélectionnez cette option pour équilibrer le trafic entre toutes les interfaces afin d'augmenter la bande passante disponible. Le routeur équilibre le trafic entre les interfaces, par permutation pondérée.
- **IP Group (By Users):** sélectionnez cette option pour regrouper le trafic sur chaque interface WAN par niveau de priorité ou par catégorie de service (CoS). Avec cette fonctionnalité, vous pouvez garantir une bande passante et un niveau de priorité plus élevé pour les services et les utilisateurs spécifiés. Tout le trafic qui n'est pas ajouté au groupeIP utilise le mode Intelligent Balancer. Pour spécifier les services et les utilisateurs, cliquez sur l'icône **Edit** pour l'interface WAN, puis ajoutez les entrées de liaison de protocole pour chaque service, adresseIP ou plage d'adressesIP.

  REMARQUE: le routeur réserve au moins un port WAN aux utilisateurs n'appartenant pas au groupeIP. Par conséquent, WAN1 est toujours configuré sur Intelligent Balancer (Auto Mode). La liaison de protocole n'est pas disponible pour WAN1.

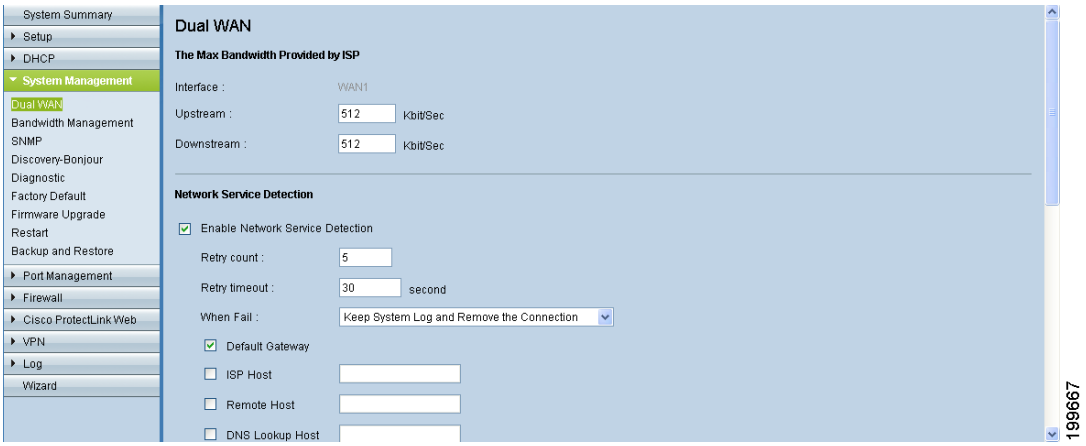
Interface Setting

Cliquez sur l'icône **Edit** correspondant à l'interface à configurer. Saisissez ensuite les paramètres de la page *Edit Dual WAN*. Pour obtenir plus d'informations, reportez-vous à **Modification des paramètres à deux et à plusieurs réseaux WAN, page 80**.

REMARQUE Si certaines modifications apportées à la page *Dual WAN* ne sont pas enregistrées, une mise en garde s'affiche. Vous pouvez cliquer sur **OK** pour fermer le message. Cliquez ensuite sur **Save** pour enregistrer vos modifications. Après avoir enregistré vos modifications, cliquez sur l'icône **Edit**. Lorsque la mise en garde s'affiche, vous pouvez également cliquer sur **Cancel** pour passer à la page de modification sans effectuer d'enregistrement.

Modification des paramètres à deux et à plusieurs réseaux WAN

La page *Dual WAN Settings* (*Multi-WAN Settings* sur le modèle RV016) apparaît dès que vous cliquez sur l'icône **Edit** d'une interface WAN, sur la page *Dual WAN* (ou *Multi-WAN*). Définissez les paramètres d'interface, selon les besoins.



REMARQUE Avant de quitter cette page, cliquez sur **Save** pour enregistrer vos paramètres ou sur **Cancel** pour les annuler. Les modifications non enregistrées ne sont pas prises en compte.

Max Bandwidth Provided by ISP:

Dans cette section, saisissez les valeurs maximales de la bande passante, telles qu'elles vous ont été communiquées par votre fournisseur d'accès à Internet. Si la bande passante excède la valeur spécifiée, le routeur utilise une autre interface WAN, pour la connexion suivante.

- **Upstream :** saisissez la bande passante maximale en amont spécifiée par votre fournisseur d'accès à Internet. La valeur par défaut est de 512kbit/s.
- **Downstream :** saisissez la bande passante maximale en aval spécifiée par votre fournisseur d'accès à Internet. La valeur par défaut est de 512kbit/s.

Network Service Detection:

Cochez éventuellement cette case pour permettre au routeur de détecter la connectivité réseau en envoyant une commande Ping aux périphériques spécifiés. Définissez ensuite les paramètres suivants. Décochez la case pour désactiver cette option.

- **Retry count** : saisissez le nombre d'envois d'une commande Ping à un périphérique. La valeur par défaut est5.

- **Retry timeout :** saisissez le nombre de secondes devant s'écouler entre deux commandes Ping. La valeur par défaut est 30secondes.
- **When Fail :** sélectionnez l'action à effectuer en cas d'échec d'un test Ping. Si vous choisissez **Generate the Error Condition in the System Log**, le routeur enregistre l'échec dans le fichier journal système. Aucun basculement n'a lieu sur l'autre interface. Si vous choisissez **Remove the Connection**, un basculement se produit et l'interface de secours est utilisée. Lorsque la connectivité du port WAN est restaurée, le trafic reprend.
- **Default Gateway, ISP Host, Remote Host** et **DNS Lookup Host :** cochez la case de chaque périphérique pour lequel vous souhaitez déterminer la connectivité réseau à l'aide d'une commande Ping. Dans le cas d'un hôte de fournisseur d'accès à Internet ou d'un hôte distant, saisissez l'adresseIP. Dans le cas d'un hôte DNS Lookup, saisissez un nom d'hôte ou un nom de domaine. Décochez la case appropriée si vous ne souhaitez pas envoyer de commande Ping à ce périphérique pour la détection d'un service réseau.

Protocol Binding (pour le modèle Cisco RV016 uniquement, lorsque l'option Load Balancer est sélectionnée):

Utilisez cette fonctionnalité pour réserver cette interface aux protocoles spécifiés, ainsi qu'aux adresses source et de destination indiquées. Si vous avez activé le mode IP Group, cette fonctionnalité n'est pas disponible.

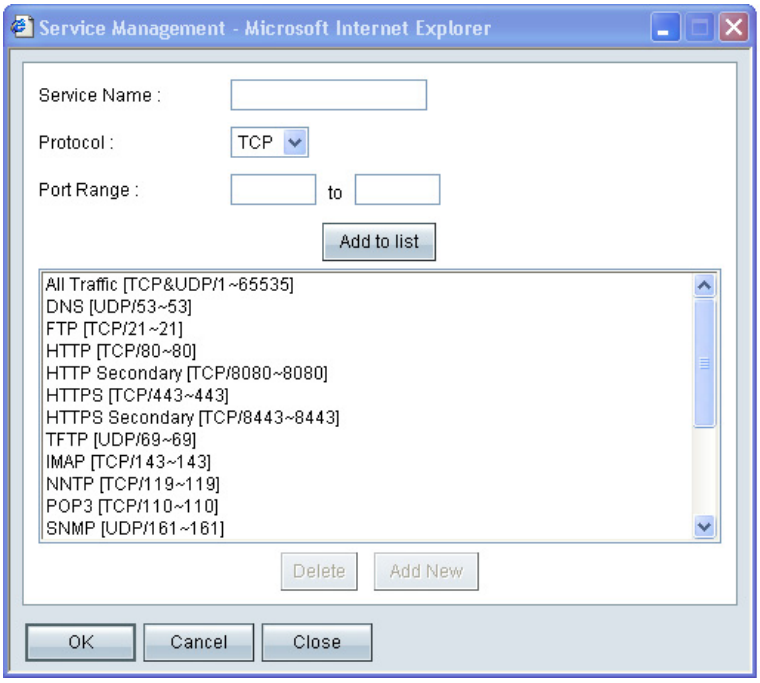
Ajoutez ou mettez à jour les entrées, selon les besoins. Notez que vos entrées ne sont pas enregistrées tant que vous n'avez pas cliqué sur le bouton Save.

- **Pour ajouter une nouvelle entrée à la liste:** saisissez les paramètres en procédant comme indiqué ci-après, puis cliquez sur **Add to list**.
  - **Service:** sélectionnez le service (ou All Traffic) à lier à cette interface WAN. Si un service particulier ne figure pas dans la liste, vous pouvez cliquer sur **Service Management** pour l'ajouter. Pour plus d'informations, reportez-vous à **Ajout d'un service, page 82**.
  - **Source IP** et **Destination IP :** spécifiez les sources internes et les destinations externes du trafic transitant par ce port WAN. Dans le cas d'une plage d'adressesIP, saisissez la première adresse dans le premier champ et la dernière, dans le champ *To*. Dans le cas d'une adresseIP unique, saisissez la même adresse dans les deux champs.
  - **Enable :** cochez ou décochez cette case pour activer ou désactiver cette règle.

- **Pour ajouter une autre entrée à la liste:** saisissez les informations, puis cliquez sur **Add to list**.
- **Pour modifier une entrée de la liste:** cliquez sur l'entrée à modifier. Les informations relatives à cet utilisateur apparaissent dans les champs de texte. Apportez les modifications voulues, puis cliquez sur **Update**. Si aucune modification n'est nécessaire, cliquez sur **Add New** pour désélectionner l'entrée et effacer le contenu des champs de texte.
- **Pour supprimer une entrée de la liste:** cliquez sur l'entrée à supprimer, puis sur **Delete**. Pour sélectionner un bloc d'entrées, cliquez sur la première entrée, maintenez la touche **Maj** enfoncée, puis cliquez sur la dernière entrée du bloc. Pour sélectionner des entrées individuellement, maintenez la touche **Ctrl** enfoncée, tout en cliquant sur chacune des entrées en question. Pour annuler la sélection d'une entrée, maintenez la touche **Ctrl** enfoncée tout en cliquant sur l'entrée.

Ajout d'un service

Pour ajouter une nouvelle entrée à la liste *Service* ou pour modifier une entrée créée précédemment, cliquez sur **Service Management**. Si le navigateur Web affiche une mise en garde relative à la fenêtre contextuelle, autorisez le contenu bloqué.



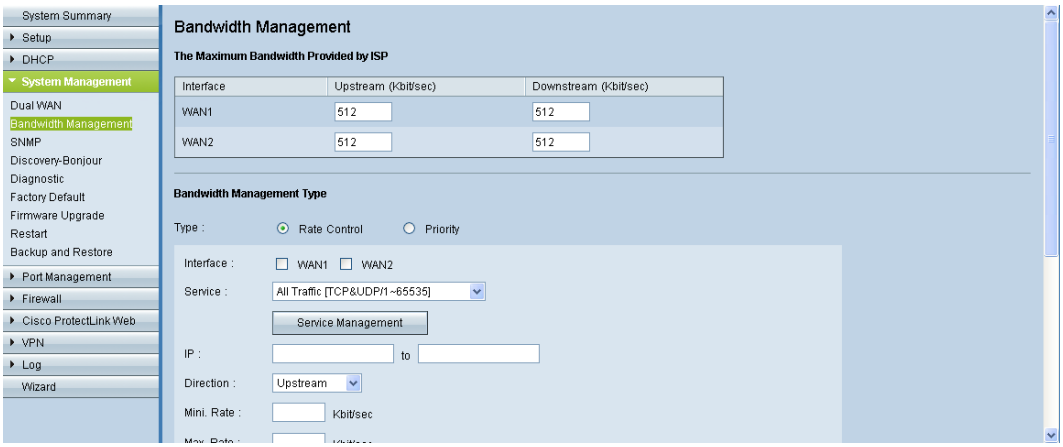
Dans la fenêtre *Service Management*, ajoutez ou mettez à jour des entrées, selon vos besoins. Avant de fermer cette fenêtre, cliquez sur **OK** pour enregistrer vos paramètres ou sur **Cancel** pour les annuler. Les modifications non enregistrées ne sont pas prises en compte.

- **Pour ajouter un service à la liste:** saisissez les informations suivantes, puis cliquez sur **Add to list**. La liste peut comporter jusqu'à 30services.
  - **Service Name :** entrez une brève description.
  - **Protocol :** sélectionnez le protocole requis. Reportez-vous à la documentation du service que vous hébergez.
  - **Port Range :** saisissez la plage de ports requise.
  - **Pour ajouter un nouveau service:** saisissez les informations, puis cliquez sur **Add to list**.
  - **Pour modifier un service que vous avez créé:** cliquez sur le service dans la liste. Les informations apparaissent dans les champs de texte. Apportez les modifications voulues, puis cliquez sur **Update**. Si aucune modification n'est nécessaire, vous pouvez cliquer sur **Add New** pour annuler la sélection du service et vider les champs de texte.
  - **Pour supprimer un service de la liste:** cliquez sur l'entrée à supprimer. Pour sélectionner un bloc d'entrées, cliquez sur la première entrée, maintenez la touche **Maj** enfoncée, puis cliquez sur la dernière entrée du bloc. Pour sélectionner plusieurs entrées individuelles, maintenez la touche **Ctrl** enfoncée tout en cliquant sur les entrées. Cliquez sur **Delete**.

Gestion des paramètres de bande passante

Utilisez la page *System Management> Bandwidth Management* pour configurer les paramètres de la bande passante du trafic en amont et en aval, ainsi que les paramètres de qualité de service (QoS) des différents types de trafic. Par exemple, vous pouvez saisir des règles de bande passante afin de garantir la qualité des services vocaux. Pour obtenir un exemple détaillé, reportez-vous à l'**Annexe F, « Gestion de la bande passante ».**

Pour ouvrir cette page: Cliquez sur **System Management > Bandwidth Management** dans l'arborescence.



REMARQUE Avant de quitter cette page, cliquez sur **Save** pour enregistrer vos paramètres ou sur **Cancel** pour les annuler. Les modifications non enregistrées ne sont pas prises en compte.

Max Bandwidth Provided by ISP

Saisissez les valeurs maximales de la bande passante, telles qu'elles vous ont été communiquées par votre fournisseur d'accès à Internet.

- **Upstream :** saisissez la bande passante maximale en amont spécifiée par votre fournisseur d'accès à Internet. La valeur par défaut est de **512**kbit/s.
- **Downstream :** saisissez la bande passante maximale en aval spécifiée par votre fournisseur d'accès à Internet. La valeur par défaut est de **12**kbit/s.

Bandwidth Management Type

Sélectionnez l'une des options de gestion suivantes:

- **Rate Control :** sélectionnez cette option afin d'indiquer les valeurs de bande passante minimale (garantie) et maximale (limitée) de chaque service ou adresseIP.
- **Priority :** sélectionnez cette option pour gérer la bande passante en identifiant les services à haute priorité et à basse priorité.

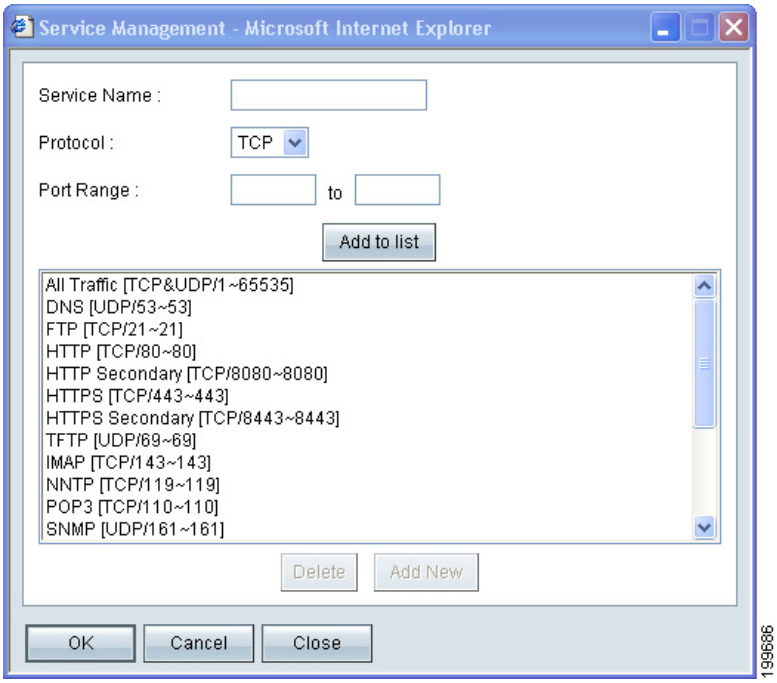
Sélectionnez une **Interface**. Ajoutez les services concernés par la gestion de la bande passante.

- **Pour ajouter un nouveau service à la liste:** Saisissez les paramètres décrits ci-après, puis cliquez sur **Add to list**. Vous pouvez ajouter jusqu'à 100services différents.
  - **Service:** sélectionnez le service à gérer. Si un service particulier ne figure pas dans la liste, vous pouvez cliquer sur **Service Management** pour l'ajouter. Pour plus d'informations, reportez-vous à **Ajout d'un service, page 86**.
  - **IP (pour l'option Rate Control uniquement):** saisissez l'adresse IP ou la plage d'adresses IP à contrôler. Pour inclure toutes les adressesIP internes, conservez la valeur par défaut.
  - **Direction :** sélectionnez **Upstream** pour le trafic sortant ou **Downstream** pour le trafic entrant.
  - **Min. Rate (pour l'option Rate Control uniquement):** saisissez le débit minimal (en Kbits/s) de la bande passante garantie.
  - **Max. Rate (pour l'option Rate Control uniquement):** saisissez le débit maximal (en Kbits/s) de la bande passante garantie.
  - **Priority (pour l'option Priority uniquement):** sélectionnez le niveau de priorité pour ce service: **High** ou **Low**.
  - **Enable :** cochez ou décochez cette case pour activer ou désactiver cette fonction.
- **Pour ajouter un autre service à la liste:** saisissez les informations, puis cliquez sur **Add to list**.
- **Pour modifier un service de la liste:** cliquez sur l'entrée à modifier. Les informations correspondantes apparaissent dans les champs de texte. Apportez les modifications voulues, puis cliquez sur **Update**. Si aucune modification n'est nécessaire, vous pouvez cliquer sur **Add New** pour annuler la sélection de l'entrée et vider les champs de texte.

- **Pour supprimer une entrée de la liste:** cliquez sur l'entrée à supprimer, puis sur **Delete**. Pour sélectionner un bloc d'entrées, cliquez sur la première entrée, maintenez la touche **Maj** enfoncée, puis cliquez sur la dernière entrée du bloc. Pour sélectionner des entrées individuellement, maintenez la touche **Ctrl** enfoncée, tout en cliquant sur chacune des entrées en question. Pour annuler la sélection d'une entrée, maintenez la touche **Ctrl** enfoncée, tout en cliquant sur l'entrée.

Ajout d'un service

Pour ajouter une nouvelle entrée à la liste *Service* ou pour modifier une entrée créée précédemment, cliquez sur **Service Management**. Si le navigateur Web affiche une mise en garde relative à la fenêtre contextuelle, autorisez le contenu bloqué.



Dans la fenêtre *Service Management*, ajoutez ou mettez à jour des entrées, selon vos besoins. Avant de fermer cette fenêtre, cliquez sur **OK** pour enregistrer vos paramètres ou sur **Cancel** pour les annuler. Les modifications non enregistrées ne sont pas prises en compte.

- **Pour ajouter un service à la liste:** saisissez les informations suivantes, puis cliquez sur **Add to List**. La liste peut comporter jusqu'à 30services.

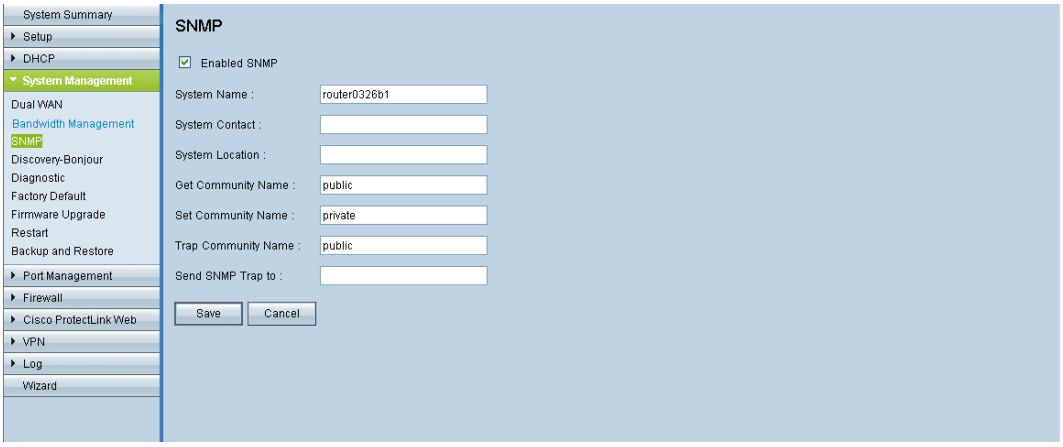
- **Service Name :** saisissez une brève description.
- **Protocol :** sélectionnez le protocole requis. Reportez-vous à la documentation du service que vous hébergez.
- **Port Range :** saisissez la plage de ports requise.

- **Pour ajouter encore un service:** saisissez les informations, puis cliquez sur **Add to list**.
- **Pour modifier un service que vous avez créé:** cliquez sur le service dans la liste. Les informations correspondantes apparaissent dans les champs de texte. Apportez les modifications voulues, puis cliquez sur **Update**. Si aucune modification n'est nécessaire, vous pouvez cliquer sur **Add New** pour annuler la sélection du service et vider les champs de texte.
- **Pour supprimer un service de la liste:** cliquez sur l'entrée à supprimer. Pour sélectionner un bloc d'entrées, cliquez sur la première entrée, maintenez la touche **Maj** enfoncée, puis cliquez sur la dernière entrée du bloc. Pour sélectionner plusieurs entrées individuelles, maintenez la touche **Ctrl** enfoncée tout en cliquant sur les entrées. Cliquez sur **Delete**.

Configuration du protocole SNMP

Utilisez la page *System Management> SNMP* pour configurer le protocole SNMP de ce routeur. Le protocole réseau SNMP (Simple Network Management Protocol) permet aux administrateurs réseau de gérer, surveiller et recevoir des notifications d'événements critiques, à mesure qu'ils se produisent sur le réseau. Le routeur prend en charge le protocole SNMPv1/v2c. Il accepte également les bases d'informations de gestion MIB (Management Information Bases) standard, telles que MIBII, ainsi que les bases MIB privées. Le routeur fait office d'agent SNMP dans la mesure où il répond aux commandes SNMP des systèmes de gestion de réseau SNMP. Il prend en charge les commandes SNMP standard, get/next/set. Il génère également des messages d'interception afin de prévenir le gestionnaire SNMP, en cas d'alarme. C'est le cas notamment lors des réinitialisations, des cycles de mise hors tension et sous tension, ainsi que lors des autres événements de la liaison du réseau étendu (WAN).

Pour ouvrir cette page: Cliquez sur **System Management> SNMP** dans l'arborescence.



REMARQUE Avant de quitter cette page, cliquez sur **Save** pour enregistrer vos paramètres ou sur **Cancel** pour les annuler. Les modifications non enregistrées ne sont pas prises en compte.

- **Enabled SNMP :** cochez cette case pour activer la fonctionnalité SNMP. Décochez-la pour désactiver cette fonctionnalité. Cette fonctionnalité est activée par défaut.
- **System Name :** définissez le nom d'hôte du routeur.
- **System Contact :** saisissez le nom de l'administrateur réseau à contacter si des mises à jour sont disponibles pour le routeur.
- **System Location :** saisissez les coordonnées de l'administrateur réseau, notamment son adresse e-mail, son numéro de téléphone ou son numéro de récepteur de radio-messagerie.
- **Get Community Name :** saisissez une chaîne de communauté pour l'authentification des commandes SNMP GET. Le nom que vous saisissez ne doit pas comporter plus de 64caractères alphanumériques. La valeur par défaut est **public**.
- **Set Community Name :** saisissez une chaîne de communauté pour l'authentification des commandes SNMP SET. Le nom que vous saisissez ne doit pas comporter plus de 64caractères alphanumériques. La valeur par défaut est **private**.
- **Trap Community Name :** créez le mot de passe qui sera envoyé avec chaque interception au gestionnaire SNMP. Le nom que vous saisissez ne doit pas comporter plus de 64caractères alphanumériques. La valeur par défaut est **public**.

- **Send SNMP Trap to (pour IPv4):** saisissez l'adresseIP ou le nom de domaine du serveur sur lequel vous exécutez le logiciel de gestion SNMP.
- **Send SNMP Trap to (pour IPv6):** ce champ est disponible à condition que l'option Dual-Stack IP soit activée dans la page *Network> Setup*. Saisissez l'adresseIPv6 ou le nom de domaine du serveur sur lequel vous exécutez le logiciel de gestion SNMP.

Activation de la détection de périphériques à l'aide du protocole Bonjour

Utilisez la page *System Management> Discovery-Bonjour* pour activer ou désactiver le protocole de détection de service Bonjour. Le protocole Bonjour permet de localiser les périphériques réseau tels que les ordinateurs et les serveurs, sur un réseau local (LAN). Les systèmes de gestion réseau que vous utilisez peuvent nécessiter cette fonctionnalité. Lorsque cette fonctionnalité est activée, le routeur diffuse à intervalles réguliers des enregistrements du service Bonjour à l'ensemble du réseau local, afin de signaler sa présence.

REMARQUE Dans le cadre de la détection des produits Cisco Small Business, Cisco fournit un utilitaire qui fonctionne via une simple barre d'outils, dans le navigateur Web. Cet utilitaire détecte les périphériques Cisco sur le réseau et affiche les informations de base les concernant, telles que leur numéro de série et leur adresseIP, afin de faciliter la configuration et le déploiement. Pour obtenir plus d'informations et télécharger l'utilitaire, visitez le site www.cisco.com/go/findit.

Pour ouvrir cette page: Cliquez sur **System Management> Discovery-Bonjour** dans l'arborescence.

Cochez la case **Enable** pour activer le protocole Bonjour. Décochez la case pour désactiver cette option. Le protocole Bonjour est activé par défaut.

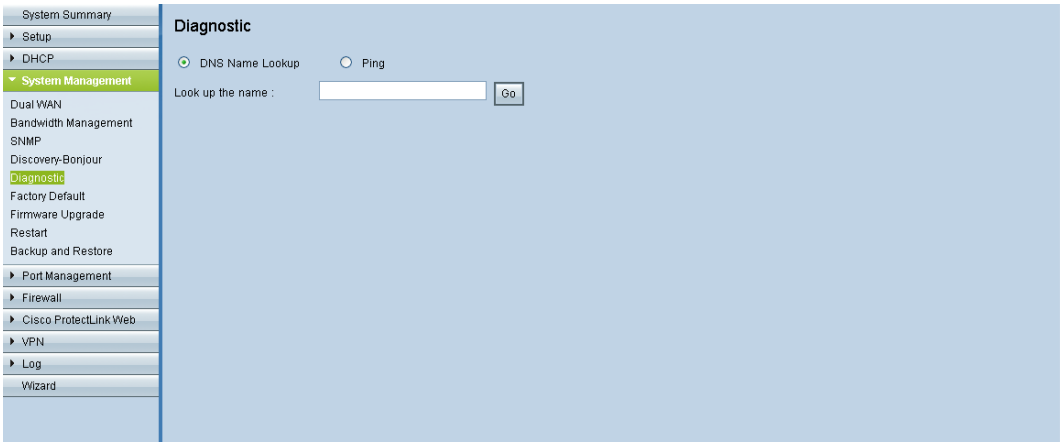
Utilisation des outils de diagnostic intégrés

Utilisez la page *System Management> Diagnostic* pour accéder à deux outils intégrés, DNS Name Lookup et Ping. Si vous suspectez un problème de connectivité, vous pouvez recourir à ces outils pour procéder à des investigations plus poussées.

Pour ouvrir cette page: cliquez sur **System Management>Diagnostic**.

Sélectionnez **DNS Name Lookup** si vous connaissez le nom d'un serveur DNS et souhaitez obtenir son adresseIP. Sélectionnez **Ping** pour tester la connectivité à une adresseIP particulière sur Internet.

DNS Name Lookup

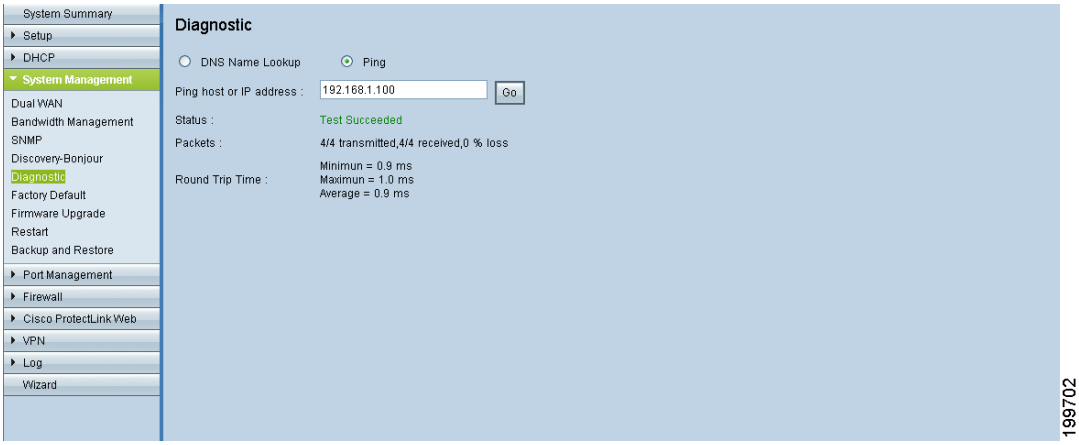


Sélectionnez cette option afin de tester la connectivité au serveur DNS que vous avez spécifié sur la page *Setup> Network* ou pour rechercher une adresseIP que vous souhaitez utiliser lors du test Ping.

Dans le champ **Look up the name**, saisissez le nom d'un hôte, comme www.cisco.com. N'incluez pas de préfixe tel que *http://.* Cliquez ensuite sur **Go**. Si le test réussit, l'adresseIP de l'hôte apparaît.

REMARQUE Cet outil s'assure que le routeur peut se connecter à un serveur DNS valide, en fonction des paramètres d'interface WAN (page *Setup> Network*).

Ping



Sélectionnez cette option pour tester la connectivité à un hôte spécifié, en saisissant l'adresseIP. Si vous ne connaissez pas l'adresseIP, faites appel à l'outil DNS Lookup pour l'obtenir. Le test Ping indique si le routeur peut envoyer un paquet à un hôte distant et recevoir une réponse de sa part. Si des utilisateurs du réseau local rencontrent des problèmes pour accéder à des services sur Internet, commencez par envoyer une commande Ping à votre serveur DNS ou à tout autre serveur dépendant de votre fournisseur d'accès à Internet. Si ce test réussit, essayez d'envoyer une commande Ping à des périphériques ne dépendant pas de votre fournisseur d'accès à Internet. Vous saurez ainsi si le problème est dû à la connexion de votre fournisseur d'accès à Internet.

Saisissez l'adresseIP, puis cliquez sur **Go**. Si le test réussit, les informations suivantes apparaissent:

- **Status :** indication permettant de savoir le test Ping est en cours d'exécution (*Testing*), s'il a réussi (*Test Succeeded*) ou s'il a échoué (*Test Failed*).
- **Packets :** nombre de paquets transmis, nombre de paquets reçus et pourcentage de paquets perdus lors du test Ping.
- **Round Trip Time :** durées minimale, maximale et moyenne des boucles lors du test Ping.

Restauration des paramètres par défaut définis en usine

Utilisez la page *System Management> Factory Default* pour effacer toutes les informations relatives à la configuration et rétablir les valeurs par défaut du routeur définies en usine. N'utilisez cette fonctionnalité que si vous souhaitez annuler l'ensemble des paramètres et préférences que vous avez configurés.

Pour ouvrir cette page: cliquez sur **System Management> Factory Default** dans l'arborescence.

STEP 1 Cliquez sur **Return to Factory Default Setting** si vous souhaitez rétablir les paramètres par défaut du routeur.

STEP 2 À l'apparition du message de confirmation, cliquez sur **OK** pour continuer. Si vous ne souhaitez pas rétablir les paramètres par défaut définis en usine, cliquez sur **Cancel**.

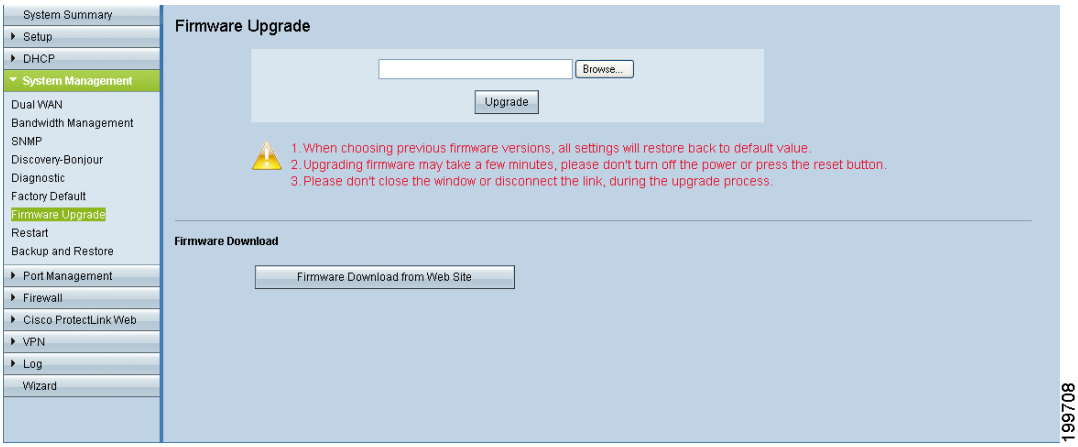
Mise à jour du microprogramme

Utilisez la page *System Management > Firmware Upgrade* pour télécharger le dernier microprogramme disponible pour votre routeur et l'installer.

AVERTISSEMENT Si vous choisissez une version antérieure du microprogramme, les paramètres par défaut sont utilisés. Tous les paramètres personnalisés sont perdus.

AVERTISSEMENT La mise à jour du microprogramme peut prendre quelques minutes. Ne mettez pas l'appareil hors tension, n'appuyez pas sur le bouton de réinitialisation, ne fermez pas le navigateur et ne mettez pas fin à la liaison au cours de ce processus.

Pour ouvrir cette page: cliquez sur **System Management > Firmware Upgrade** dans l'arborescence.



Procédez comme suit:

- **Pour effectuer la mise à niveau à partir d'un fichier de microprogramme sur votre ordinateur:** cliquez sur **Browse** et choisissez le fichier extrait. Cliquez sur **Firmware Upgrade Right Now**. Quelques minutes plus tard, le message de réinitialisation apparaît. Patientez environ une minute, le temps que le navigateur soit actualisé. Si le navigateur n'affiche pas automatiquement la page de connexion, vous devrez peut-être saisir une nouvelle fois l'adresseIP dans la barre d'adresse du navigateur. Si votre PC

ne parvient pas à se reconnecter à l'utilitaire de configuration, vous devrez peut-être libérer votre adresseIP, puis la restaurer.

- **Pour télécharger la dernière version du microprogramme sur le site de Cisco:** cliquez sur **Firmware Download from Web Site**. Votre navigateur Web affiche la page d'informations sur le routeur sur le site Cisco.com. Cliquez sur le bouton **Download Firmware**. Passez tous les écrans en revue afin de sélectionner la dernière version du microprogramme du routeur, puis téléchargez le fichier correspondant. Extrayez le fichier sur votre ordinateur. Procédez ensuite à la mise à niveau du microprogramme, comme décrit précédemment.

Redémarrage du routeur

Si vous devez redémarrer le routeur, Cisco recommande d'utiliser l'outil Restart sur cette page. Lorsque vous effectuez un redémarrage à partir de la page *System Management> Restart*, le routeur vous fait parvenir un fichier journal (si la consignation est activée), avant la réinitialisation.

Pour ouvrir cette page: cliquez sur **System Management> Restart** dans l'arborescence.

STEP 1 Cliquez sur **Restart Router** pour redémarrer le routeur.

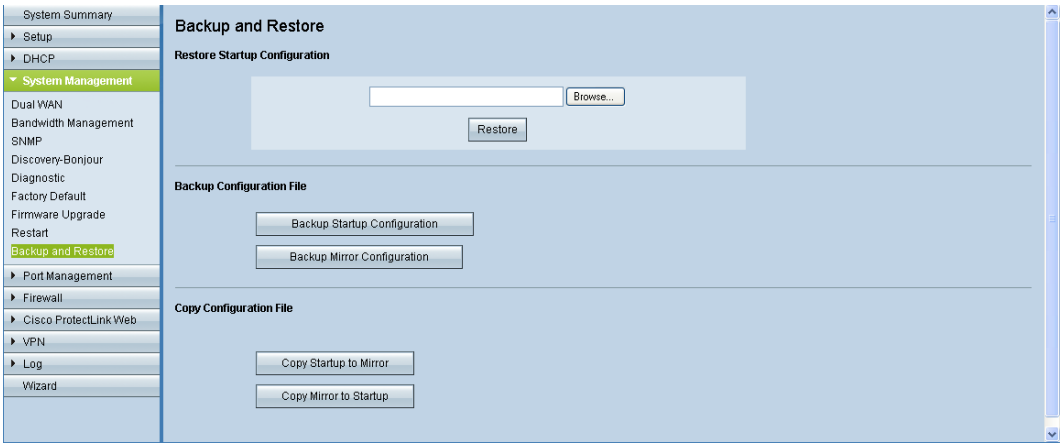
STEP 2 À l'apparition du message de confirmation, cliquez sur **OK** pour continuer. Si vous ne souhaitez pas redémarrer le routeur, cliquez sur **Cancel**.

Sauvegarde et restauration des paramètres

Utilisez la page *System Management> Backup and Restore* pour importer, exporter et copier vos fichiers de configuration. Le routeur propose deux fichiers de configuration: le fichier de démarrage et le fichier miroir. Le fichier de démarrage désigne le fichier de configuration que le routeur charge lors d'un démarrage. Le routeur copie automatiquement le fichier de démarrage dans le fichier miroir. De ce fait, le fichier miroir contient les dernières informations de configuration valides connues. Par la suite, si le fichier de configuration de démarrage est altéré, pour une raison quelconque, il est possible de recourir au fichier de configuration miroir.

REMARQUE Le routeur copie automatiquement le fichier de configuration de démarrage dans le fichier de configuration miroir, après 24heures d'exécution dans des conditions stables (aucun redémarrage et aucun changement de configuration au cours des dernières 24heures).

Pour ouvrir cette page: cliquez sur **System Management > Backup and Restore** dans l'arborescence.



Vous pouvez effectuer les tâches suivantes:

- **Restauration des paramètres à partir d'un fichier de configuration, page 96**
- **Sauvegarde des fichiers de configuration et des fichiers miroir, page 96**
- **Copie d'un fichier de démarrage ou d'un fichier miroir, page 96**

Restauration des paramètres à partir d'un fichier de configuration

Si vous souhaitez rétablir les paramètres enregistrés précédemment, il est possible d'importer un fichier de configuration.

STEP 1 Dans la section *Restore Startup Configuration File*, cliquez sur **Browse**.

STEP 2 Sélectionnez un fichier de configuration (.config).

STEP 3 Cliquez sur **Restore**. Ce processus peut prendre jusqu'à une minute.

STEP 4 Cliquez sur **System Management> Restart** dans l'arborescence.

STEP 5 À l'apparition du message de confirmation, cliquez sur **OK**. Si vous ne souhaitez pas redémarrer le routeur, cliquez sur **Cancel**. Les paramètres importés ne sont appliqués qu'après le redémarrage du routeur.

REMARQUE: vous pouvez également utiliser le bouton Restart. Appuyez sur le bouton **Restart** et maintenez-le enfoncé pendant une seconde, puis relâchez-le pour redémarrer le routeur.

Sauvegarde des fichiers de configuration et des fichiers miroir

Vous avez la possibilité d'enregistrer les fichiers de configuration de démarrage et miroir sur votre ordinateur. Si nécessaire, vous pouvez utiliser ces fichiers pour restaurer les paramètres.

STEP 1 Cliquez sur **Backup Startup Configuration** ou sur **Backup Mirror Configuration**.

STEP 2 Lorsque la fenêtre *File Download* apparaît, cliquez sur **Save**, puis choisissez l'emplacement du fichier. Vous pouvez éventuellement saisir un nom de fichier descriptif. Cliquez ensuite sur **Save**.

CONSEIL: les noms de fichier par défaut sont respectivement *Startup.config* et *Mirror.config*. Il peut être utile de saisir un nom de fichier incluant la date et l'heure actuelles, afin de faciliter l'identification lors de la prochaine importation d'un fichier.

STEP 3 Fermez la fenêtre *Download Complete*.

Copie d'un fichier de démarrage ou d'un fichier miroir

Si nécessaire, vous pouvez copier manuellement votre fichier de configuration de démarrage dans votre fichier de configuration miroir, ou inversement.

CONSEIL Ce processus permet, par exemple, de sauvegarder une configuration connue avant d'effectuer des modifications. Copiez le fichier de démarrage dans le fichier miroir avant d'effectuer vos modifications. Si les modifications que vous avez apportées ne vous conviennent pas, copiez le fichier miroir dans le fichier de démarrage, afin de restaurer les paramètres.

REMARQUE

- Le fichier de configuration de démarrage est automatiquement copié dans le fichier de configuration miroir toutes les 24heures.
- En cas de modification d'un paramètre, le compteur horaire est réinitialisé et la prochaine copie automatique a lieu 24heures plus tard.
- Si le fichier de configuration miroir se trouve toujours dans l'état par défaut, la copie de ce fichier dans le fichier de démarrage restaure immédiatement les paramètres par défaut définis en usine du routeur.

Pour copier un fichier, cliquez sur le bouton:

- **Copy Startup to Mirror :** cliquez sur ce bouton pour remplacer le fichier miroir par le fichier de démarrage. L'opération de copie est exécutée immédiatement et il n'est pas possible de l'annuler. À l'issue de l'opération, la page du navigateur est actualisée.
- **Copy Mirror to Startup :** cliquez sur ce bouton pour remplacer le fichier de démarrage par le fichier miroir. L'opération de copie est exécutée immédiatement et il n'est pas possible de l'annuler. Après un bref instant, le routeur redémarre. Si votre PC ne parvient pas immédiatement à recharger la page de connexion, saisissez de nouveau l'adresseIP de l'utilitaire de configuration, dans la barre d'adresse. Puis connectez-vous.

6

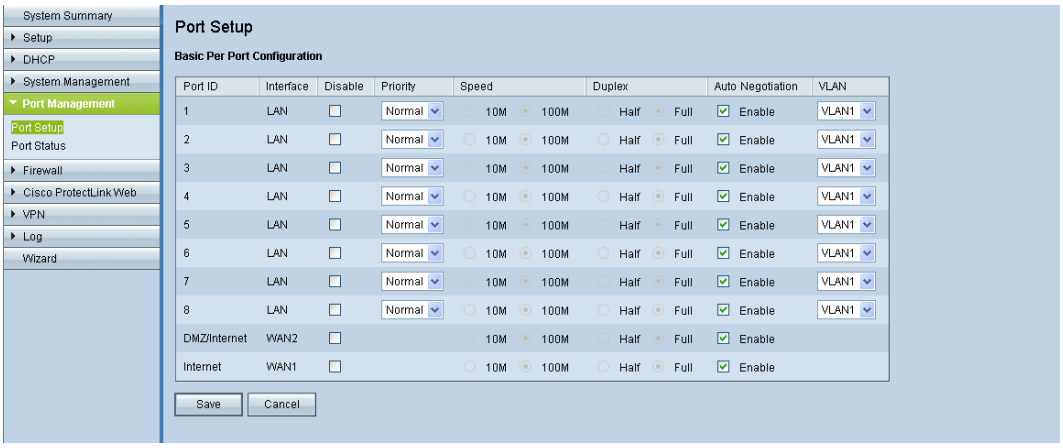
Gestion des ports

Utilisez le module Port Management pour configurer les paramètres de port et afficher le statut des ports.

Configuration des paramètres de port

Les paramètres de port par défaut devraient être suffisants pour la plupart des petites et moyennes entreprises. Vous pouvez toutefois utiliser la page *Port Management> Port Setup* pour les personnaliser, si nécessaire. Vous pouvez désactiver un port ou en changer la priorité, la vitesse, le mode duplex et les paramètres de négociation. Vous pouvez également activer des réseaux VLAN (Virtual Local Area Network, réseau local virtuel) basés sur les ports pour contrôler le trafic entre les périphériques de votre réseau.

Pour ouvrir cette page: Cliquez sur **Port Management> Port Setup** dans l'arborescence.



REMARQUE Avant de quitter cette page, cliquez sur **Save** pour enregistrer vos paramètres ou sur **Cancel** pour les annuler. Les modifications non enregistrées ne sont pas prises en compte.

Pour le routeur CiscoRV016 uniquement, choisissez le nombre de ports WAN dans la liste déroulante ou conservez la valeur par défaut (2). Si vous changez le nombre de ports, enregistrez vos paramètres. (Vous pouvez également changer le nombre de ports WAN à la page *Setup> Network*.)

Les informations en lecture seule qui suivent sont affichées pour chaque port:

- **Port ID :** numéro ou nom du port indiqué sur le périphérique.
- **Interface :** type d'interface : LAN, WAN ou DMZ.

Saisissez les paramètres suivants, si nécessaire:

- **Disable :** cochez cette case pour désactiver un port. Par défaut, tous les ports sont activés.
- **Priority** (pour les ports LAN uniquement) **:** utilisez ce paramètre pour garantir la qualité de service en donnant la priorité au trafic des périphériques branchés sur des ports spécifiques. Par exemple, vous pouvez attribuer une priorité élevée à un port utilisé pour les jeux ou pour la vidéoconférence. Pour chaque port, sélectionnez le niveau de priorité approprié, **High** ou **Normal**. Le paramètre par défaut est Normal.
- **Speed :** pour régler ce paramètre, vous devez d'abord décocher la case **Enable** dans la colonne *Auto Neg*, afin de désactiver la négociation automatique. Sélectionnez ensuite la vitesse du port: **10M** ou **100M**.
- **Duplex :** pour définir le mode duplex, vous devez d'abord décocher la case **Enable** dans la colonne *Auto Neg*, afin de désactiver la négociation automatique. Sélectionnez le mode duplex: **Half** ou **Full**.
- **Auto Neg. :** cochez la case **Enable** pour permettre au routeur de négocier automatiquement les vitesses de connexion et le mode duplex. Cette fonctionnalité est activée par défaut.
- **VLAN** (pour les ports LAN uniquement) **:** par défaut, tous les ports LAN sont sur le réseau VLAN1. Pour placer un port sur un réseau VLAN distinct, choisissez un réseau VLAN dans la liste déroulante.

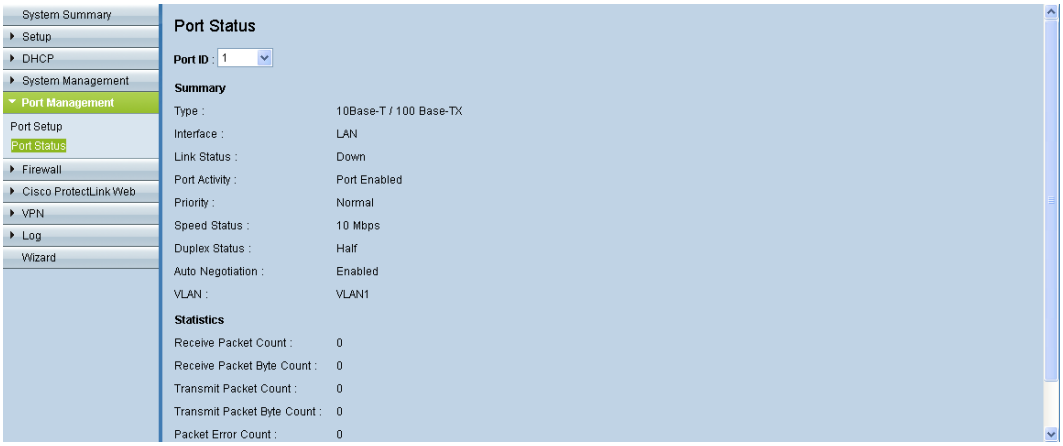
  Le nombre de réseaux VLAN disponibles est égal au nombre de ports LAN: 4sur le routeur Cisco RV042 et RV042G, 8sur le routeur Cisco RV082 et jusqu'à13 sur le routeur Cisco RV016 (selon l'utilisation des ports à double fonction). Par exemple, vous pouvez avoir un commutateur Ethernet, sur le port4, qui fournit la connectivité Internet aux utilisateurs invités dans une

salle de conférence. Pour empêcher vos invités d'accéder aux serveurs de fichiers et aux imprimantes de votre réseau LAN, vous pouvez placer le port4 sur le réseau VLAN2 et laisser les autres ports sur le réseau VLAN1. Il n'y a pas de communication entre les périphériques situés sur des réseaux VLAN distincts.

Affichage des informations sur l'état d'un port

Utilisez la page *Port Management> Port Status* pour visualiser les informations et les statistiques relatives à un port donné.

Pour ouvrir cette page: Cliquez sur **Port Management> Port Status** dans l'arborescence.



Dans la liste **Port ID**, choisissez un port. Vous pouvez cliquer sur **Refresh** pour mettre à jour les données.

Summary

Les informations suivantes sur le port sélectionné sont affichées dans la section Summary:

- **Type :** type de port.
- **Interface :** type d'interface, à savoir LAN ou WAN.
- **Link Status :** état de la connexion.
- **Port Activity :** état du port.

- **Speed Status :** vitesse du port : 10Mbit/s (10Mbps) ou 100Mbit/s (100Mbps).
- **Duplex Status :** mode duplex : semi-duplex (*Half*) ou duplex intégral (*Full*).
- **Auto negotiation :** état de la fonctionnalité de négociation automatique.
- **VLAN :** VLAN auquel appartient le port.

Statistics

Les informations suivantes sur le port sélectionné sont affichées dans la section Statistics:

- **Port Receive Packet Count :** nombre de paquets reçus.
- **Port Receive Packet Byte Count :** nombre d'octets de paquets reçus.
- **Port Transmit Packet Count :** nombre de paquets transmis.
- **Port Transmit Packet Byte Count :** nombre d'octets de paquets transmis.
- **Port Packet Error Count :** nombre d'erreurs de paquets.

7

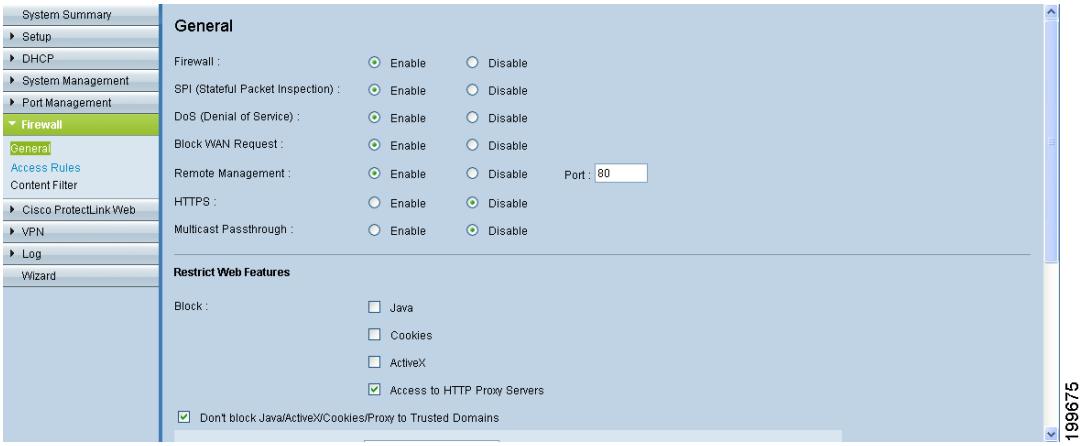
Pare-feu

Utilisez le module Firewall pour configurer les fonctionnalités de pare-feu, créer des règles d'accès et définir des filtres de contenu pour contrôler les activités de vos utilisateurs sur Internet. Reportez-vous aux rubriques suivantes:

Configuration des paramètres de pare-feu généraux

Les paramètres de pare-feu par défaut sont généralement suffisants pour la plupart des petites et moyennes entreprises. Vous pouvez toutefois utiliser la page *Firewall > General* pour désactiver le pare-feu ou pour indiquer les types d'attaques que vous souhaitez bloquer. Vous pouvez également interdire les fonctionnalités de site Web potentiellement dangereuses, comme Java et les cookies.

Pour ouvrir cette page : Cliquez sur **Pare-feu > General** dans l'arborescence.



REMARQUE

- La désactivation du pare-feu (non recommandée) n'est possible que si vous avez configuré le mot de passe de l'administrateur. Si vous utilisez toujours le mot de passe par défaut, vous devez le changer. Pour obtenir plus d'informations, reportez-vous à **Changement du nom d'utilisateur et du mot de passe de l'administrateur, page 42**.
- Avant de quitter cette page, cliquez sur **Save,** pour enregistrer les paramètres ou sur **Cancel,** pour les annuler. Les modifications non enregistrées ne sont pas prises en compte.

Activez ou désactivez le pare-feu et les fonctionnalités associées:

- **Firewall :** cette option sert à activer ou à désactiver le pare-feu. Cette fonctionnalité est activée par défaut. Elle est vivement recommandée, pour protéger votre réseau. L'activation ou la désactivation du pare-feu affectent également plusieurs fonctionnalités associées, comme décrit ci-après. La désactivation du pare-feu entraîne la désactivation des règles d'accès et des filtres de contenu.

  Si vous choisissez **Disable** et que vous utilisez toujours le mot de passe de l'administrateur par défaut, un message apparaît. Pour protéger votre routeur contre les accès non autorisés, vous devez changer le mot de passe pour pouvoir désactiver le pare-feu. Cliquez sur **OK** pour passer à la page *Password* ou cliquez sur **Cancel**, pour rester sur la page actuelle. Une fois que votre mot de passe a été modifié, vous pouvez revenir à cette page et poursuivre la procédure.

- **SPI (Stateful Packet Inspection):** lorsque cette fonctionnalité est activée, le routeur examine les informations qui passent à travers le pare-feu. Il inspecte tous les paquets en fonction de la connexion établie, avant de transmettre les paquets à une couche supérieure de protocole, en vue de

leur traitement. Cette fonctionnalité ne peut être activée que lorsque le pare-feu est activé.

- **DoS (Denial of Service) :** lorsqu'elle est activée, cette fonctionnalité protège les réseaux internes contre les attaques par Internet. Elles peuvent prendre les formes suivantes: inondations SYN, attaques par réflexion (Smurf), attaques sur le terrain (LAND), Ping fatal, usurpation d'adresse IP et attaques par réassemblage. Cette fonctionnalité ne peut être activée que lorsque le pare-feu est activé.
- **Block WAN Requests :** lorsque cette fonctionnalité est activée, le routeur abandonne les requêtes TCP et les paquets ICMP non acceptés provenant du réseau WAN. Les pirates informatiques ne peuvent pas trouver le routeur en effectuant un test Ping de l'adresse IP WAN. Cette fonctionnalité ne peut être activée que lorsque le pare-feu est activé.
- **Gestion à distance :** lorsque cette fonctionnalité est activée, vous pouvez vous connecter à l'utilitaire Web de configuration du routeur par le biais d'une connexion WAN. Par défaut, cette fonction est désactivée. Elle ne peut être activée que lorsque le pare-feu est activé. Pour activer la gestion à distance, vous devez d'abord configurer un mot de passe d'administrateur sécurisé, à la page *Setup > Password*. Cela empêche les utilisateurs non autorisés d'accéder au routeur à l'aide du mot de passe par défaut. Lorsque vous activez cette fonctionnalité, vous pouvez conserver le paramètre par défaut **Port**, soit 80 ou saisir un autre numéro de port (en général, 8080).

  REMARQUE: lorsque la gestion à distance est activée, vous pouvez utiliser un navigateur Web pour accéder à l'utilitaire de configuration de n'importe quelle zone d'Internet. Dans le navigateur Web, saisissez **http://<adresse IP WAN du routeur>:port** ou **https://<adresse IP WAN du routeur>:port**, si vous avez activé la fonctionnalité HTTPS.
- **HTTPS:** lorsqu'elle est activée, cette fonctionnalité autorise les sessions HTTP sécurisées. Cette fonctionnalité est activée par défaut.

  REMARQUE: si vous désactivez la fonctionnalité HTTPS, les utilisateurs ne pourront pas se connecter à l'aide de QuickVPN.
- **Multicast Pass Through:** lorsqu'elle est activée, cette fonctionnalité permet la transmission des paquets multidestination aux périphériques LAN appropriés. Le transfert multidiffusion est utilisé pour les jeux Internet, la vidéoconférence et les applications multimédias. Cette option est désactivée par défaut.

IMPORTANT : ce routeur ne prend pas en charge le passage de trafic multidiffusion sur un tunnel IPSec. L'option de transfert multidiffusion détermine si le routeur permet au trafic multidiffusion provenant d'Internet de passer à travers le pare-feu, pour être transmis au réseau LAN.

Restrict WEB Features

- **Java:** cochez cette case pour que le pare-feu bloque les applets Java. Java est un langage de programmation commun pour sitesWeb. Si vous bloquez les applets Java, vous risquez de ne pas avoir accès aux sites Internet créés à l'aide de ce langage de programmation. Pour remédier à ce problème, cochez cette case, pour bloquer Java sur les sites non autorisés ou inconnus et autorisez Java sur les sites de confiance (reportez-vous à *Don't block Java/Java/ActiveX/Cookies/Proxy to Trusted Domains*, ci-après). Par défaut, Java n'est pas bloqué.
- **Cookies:** cochez pour que le pare-feu bloque tous les cookies. Les cookies sont des données stockées par un site Web sur l'ordinateur d'un utilisateur. Si vous bloquez les cookies, les sites Web risquent de ne pas fonctionner comme prévu. Pour remédier à ce problème, cochez cette case, pour bloquer les cookies sur les sites non autorisés ou inconnus et autorisez-les sur les sites de confiance (reportez-vous à *Don't block Java/Java/ActiveX/Cookies/Proxy to Trusted Domains*, ci-après). Par défaut, les cookies ne sont pas bloqués.
- **ActiveX:** cochez cette case pour que le pare-feu bloque les contrôles ActiveX. ActiveX est un langage de programmation pour sitesWeb. Si vous interdisez ActiveX, vous risquez de ne pas avoir accès aux sites Internet créés à l'aide de ce langage de programmation. Pour remédier à ce problème, cochez cette case, pour bloquer les contrôles ActiveX sur les sites non autorisés ou inconnus et autorisez-les sur les sites de confiance (reportez-vous à *Don't block Java/Java/ActiveX/Cookies/Proxy to Trusted Domains*, ci-après). Par défaut, les contrôles ActiveX ne sont pas bloqués.
- **Access to HTTP Proxy Servers :** cochez cette case pour bloquer l'accès aux serveurs proxy HTTP. L'utilisation de serveurs proxy WAN peut compromettre la sécurité du routeur. En activant cette fonctionnalité, vous bloquez l'accès aux serveurs proxy qui utilisent les ports 80 ou 8080. Pour remédier à ce problème, cochez cette case, pour bloquer l'accès aux serveurs non autorisés ou inconnus et autorisez l'accès aux serveurs de confiance (reportez-vous à *Don't block Java/Java/ActiveX/Cookies/Proxy to Trusted Domains* ci-après). Par défaut, l'accès aux serveurs proxy HTTP est autorisé.
- **Don't block Java/ActiveX/Cookies/Proxy to Trusted Domains:** si vous avez désactivé l'une des fonctionnalités Web, vous pouvez cocher cette case pour activer ces fonctionnalités pour les domaines que vous ajoutez à

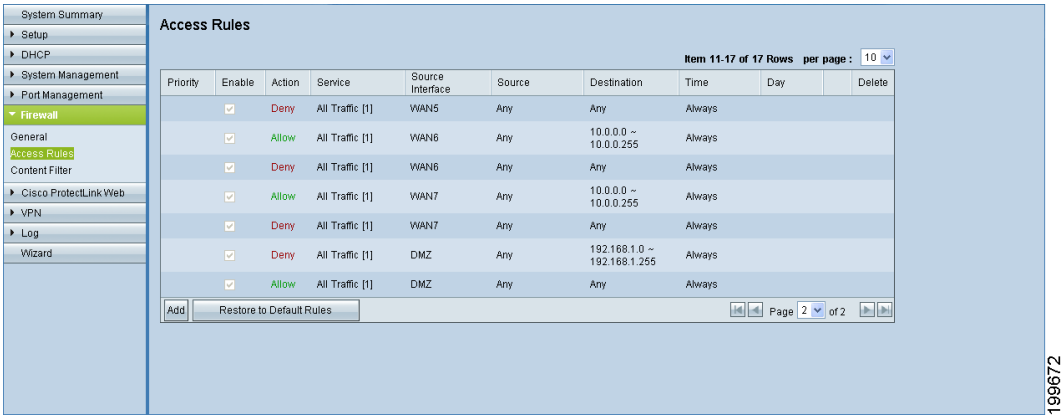
la liste de confiance. (Cette zone de la page n'est disponible que si vous avez coché l'une des autres cases, pour désactiver une fonctionnalité Web.) Si vous laissez la case désactivée, les fonctionnalités Web seront désactivées pour tous les sites Web.

- **Pour ajouter un domaine à la liste de confiance :** saisissez le nom du domaine à ajouter à la liste de confiance. Puis cliquez sur **Add to list**.
- **Pour ajouter un autre domaine à la liste de confiance:** indiquez le domaine, puis cliquez sur **Add to list**.
- **Pour modifier un domaine dans la liste de confiance:** cliquez sur le domaine. Les informations apparaissent dans le champ de texte. Effectuez les modifications et cliquez sur **Update**.
- **Pour supprimer un domaine de la liste de confiance:** Cliquez sur le domaine, puis cliquez sur **Delete**.

Configuration des règles d'accès au pare-feu

Les règles d'accès par défaut sont généralement suffisantes pour la plupart des petites et moyennes entreprises. Vous pouvez toutefois utiliser la page *Firewall > Access Rules* pour modifier ou ajouter de nouvelles règles d'accès, pour votre réseau. Les règles d'accès déterminent le trafic qui est autorisé à passer à travers le pare-feu du routeur. Facultatif: vous pouvez définir un calendrier pour activer ou désactiver chaque règle d'accès, à des dates et à des heures données.

Pour ouvrir cette page : Cliquez sur **Pare-feu > Access Rules** dans l'arborescence.



REMARQUE Avant de quitter cette page, cliquez sur **Save** pour enregistrer vos paramètres ou sur **Cancel**, pour les annuler. Les modifications non enregistrées ne sont pas prises en compte.

Reportez-vous aux rubriques suivantes:

- **À propos des règles d'accès, page 107**
- **Gestion des règles d'accès, page 108**
- **Configuration des règles d'accès, page 110**

À propos des règles d'accès

Les règles par défaut suivantes sont définies pour le routeur:

- Tout le trafic du réseau LAN vers le réseau WAN est autorisé.
- Tout le trafic du réseau WAN vers le réseau LAN est interdit.
- Tout le trafic du réseau LAN vers le réseau DMZ est autorisé.
- Tout le trafic du réseau DMZ vers le réseau LAN est interdit.
- Tout le trafic du réseau WAN vers le réseau DMZ est autorisé.
- Tout le trafic du réseau DMZ vers le réseau WAN est autorisé.

ATTENTION Avec l'utilisation de règles personnalisées, il est possible de désactiver la protection par pare-feu ou de bloquer tous les accès à Internet. Par conséquent, soyez très prudent lorsque vous créez ou supprimez des règles d'accès.

Quatre règles par défaut additionnelles sont toujours actives et ne peuvent être remplacées par aucune règle personnalisée:

- Le service HTTP en provenance du réseau LAN vers le routeur est toujours autorisé.
- Le service DHCP en provenance du réseau LAN est toujours autorisé.
- Le service DNS en provenance du réseau LAN est toujours autorisé.
- Le service Ping en provenance du réseau LAN vers le routeur est toujours autorisé.

Gestion des règles d'accès

À l'exception des règles par défaut, toutes les règles d'accès configurées sont répertoriées dans le tableau des règles d'accès et vous pouvez définir la priorité de chaque règle personnalisée.

Cliquez sur l'onglet **IPv4** pour définir les règles du trafic comportant des adresses IPv4 ou cliquez sur l'onglet **IPv6** pour définir les règles du trafic comportant des adresses IPv6.
Remarque: L'onglet IPv6 n'est disponible que si vous avez activé l'adresse IP Dual-Stack dans la page *Network* > *Setup*.

REMARQUE À la place de cette procédure, vous pouvez utiliser l'assistant Access Rule Wizard. Pour obtenir plus d'informations, reportez-vous au **Chapitre 11, « Assistant ».**

Si vous disposez de nombreuses règles, vous pouvez ajuster l'affichage. Utilisez l'option *Rows per page list,* située dans le coin supérieur droit du tableau, pour choisir le nombre de règles à afficher sur chaque page. Utilisez la liste *Page,* située au-dessous du tableau, pour choisir une page spécifique. Utilisez les boutons de navigation pour afficher la première page, la page précédente, la page suivante ou la dernière page. Selon le nombre de pages dont vous disposez et la sélection actuelle, certains boutons risquent de ne pas être disponibles.

- **Priority :** priorité de la règle d'accès, 1 correspondant à la priorité la plus élevée. Pour modifier la priorité d'une règle, sélectionnez une option, dans la liste déroulante. S'il existe un conflit entre deux règles d'accès, la règle de priorité supérieure l'emporte. Les règles d'accès par défaut ont la plus basse priorité.

  Lorsqu'une règle d'accès est créée, le routeur lui attribue automatiquement une priorité; vous pouvez toutefois changer la priorité de la règle après la création de cette dernière.

- **Enable:** pour activer une règle, cochez la case **Enable**. Pour désactiver la règle, décochez la case. Les règles par défaut ne peuvent pas être modifiées.

Des informations additionnelles ne pouvant pas être modifiées sont affichées sur cette page:

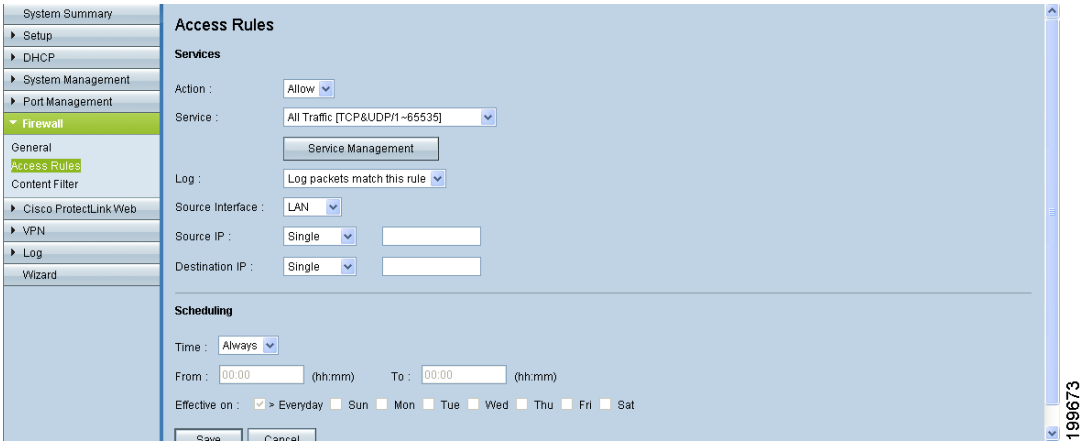
- **Action:** action effectuée par la règle (autoriser ou refuser l'accès)
- **Service:** service affecté par la règle
- **Source Interface :** interface source affectée par la règle
- **Source:** adresse IP de la source du trafic ou aucune

- **Destination :** adresse IP de la destination du trafic ou aucune
- **Time:** durée spécifique pendant laquelle la règle d'accès est active ou toujours
- **Day :** jours spécifiques pendant lesquels la règle d'accès est active ou toujours

Ajoutez ou modifiez des règles, selon les besoins.

- **To add a rule :** Cliquez sur **Add New Rule**. Entrez les paramètres, comme décrit à la section **Configuration des règles d'accès, page 110**.
- **Pour modifier un règle personnalisée:** Cliquez sur l'icône **Edit**. Entrez les paramètres, comme décrit à la section **Configuration des règles d'accès, page 110**.
- **Pour supprimer une règle d'accès :** Cliquez sur l'icône **Delete**. Lorsque le message de confirmation apparaît, cliquez sur **OK** pour continuer ou sur **Cancel**, pour fermer la fenêtre de message sans supprimer la règle.
- **Pour supprimer toutes les règles personnalisées:** Cliquez sur **Restore to Default Rules**.

Configuration des règles d'accès



Après avoir cliqué sur l'icône **Add New Rule** ou **Edit** dans le tableau *Access Rules*, saisissez les informations suivantes, sur la page d'ajout/de modification.

REMARQUE Avant de quitter cette page, cliquez sur **Save** pour enregistrer vos paramètres. Lorsque le message de réussite apparaît, cliquez sur **OK** pour rester sur la page actuelle et ajouter une autre règle d'accès ou cliquez sur **Cancel** pour revenir au tableau *Access Rules*. Pour annuler les modifications que vous avez apportées sur cette page, cliquez sur **Cancel**. Les modifications non enregistrées ne sont pas prises en compte.

Services (IPv4 et IPv6)

- **Action:** sélectionnez l'action effectuée par la règle afin d'autoriser ou de refuser l'accès.
- **Service:** sélectionnez le service concerné par cette règle. Si vous devez ajouter un service, cliquez sur **Service Management**. Pour plus d'informations, reportez-vous à **Ajout d'un service, page 112**.
- **Log :** pour inclure des événements pour cette règle dans le journal, cliquez sur **Log packets match this rule**. Sinon, cliquez sur **Not log**. Ce paramètre prend effet à condition que la consignation soit activée. Pour plus d'informations, reportez-vous au **Chapitre 10, « Surveillance des statistiques du système »**..
- **Source Interface :** sélectionnez l'interface source concernée par cette règle.

- **Source IP (IPv4)** ou **Source IP / Prefix Length (IPv6):** identifiez la source de trafic concernée par cette règle. Choisissez une des options suivantes dans la liste déroulante:
  - **Single :** cette règle s'applique à une seule adresse IP. Saisissez l'adresseIP.
  - **Range :** cette règle s'applique à une plage d'adresses IP (IPv4 uniquement). Saisissez l'adresseIP de début de la plage dans la première case, puis l'adresseIP de fin de la plage dans la deuxième case.
  - **Subnet :** cette règle s'applique à un sous-réseau (IPv6 uniquement). Saisissez l'adresseIP et la longueur du préfixe.
  - **ANY :** cette règle s'applique à n'importe quelle adresseIP.
- **Destination IP (IPv4)** ou **Destination IP/ Prefix Length (IPv6):** identifiez la destination de trafic concernée par cette règle. Choisissez une des options suivantes dans la liste déroulante:
  - **Single :** cette règle s'applique à une seule adresse IP. Saisissez l'adresseIP.
  - **Range :** cette règle s'applique à une plage d'adresses IP (IPv4 uniquement). Saisissez l'adresseIP de début de la plage dans la première case, puis l'adresseIP de fin de la plage dans la deuxième case.
  - **Subnet :** cette règle s'applique à un sous-réseau (IPv6 uniquement). Saisissez l'adresseIP et le numéro de notation CIDR du sous-réseau.
  - **ANY :** cette règle s'applique à n'importe quelle adresseIP.

Schedule (IPv4 uniquement) :

Conservez les paramètres par défaut ou programmez la période d'activation de cette règle:

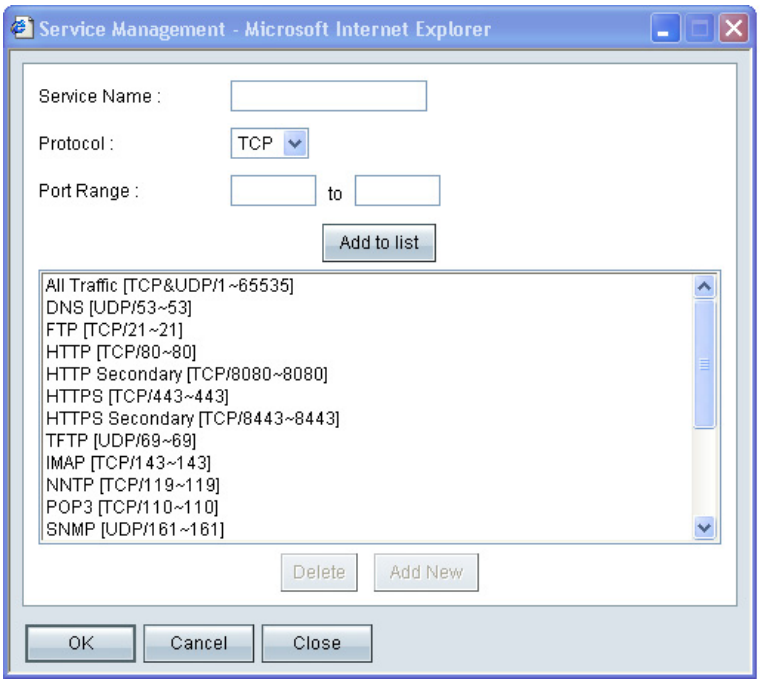
- **Time:** sélectionnez l'une des options suivantes:
  - **Always :** sélectionnez cette option si la règle s'applique tout le temps, tous les jours de la semaine. Vous pouvez éventuellement saisir une période dans les champs *From* et *To*.
  - **Interval :** sélectionnez cette option pour spécifier la période pendant laquelle la règle est active. Si vous choisissez cette option, vous devez

saisir une période dans les champs *From* et *To*. Vous pouvez éventuellement spécifier les jours de la semaine.

- **From** et **To :** si vous choisissez Interval, utilisez ces champs pour spécifier les heures et les jours d'activation de la règle. Saisissez l'heure de début dans le champ *From* et l'heure de fin, dans le champ *To*. Utilisez le format hh:mm (15:30 correspond à 15h30). Saisissez 00:00 à 00:00 si la règle s'applique à toutes les heures du jour.
- **Effective on :** si vous choisissez Interval, utilisez ces cases pour spécifier les jours pendant lesquels la règle est active. Cochez la case **Everyday** si la règle est active tous les jours. Pour sélectionner des jours spécifiques, décochez la case **Everyday**, puis activez la case correspondant à chaque jour d'activation de la règle.

Ajout d'un service

Pour ajouter une nouvelle entrée à la liste *Service* ou pour modifier une entrée créée précédemment, cliquez sur **Service Management**. Si le navigateur Web affiche une mise en garde relative à la fenêtre contextuelle, autorisez le contenu bloqué.



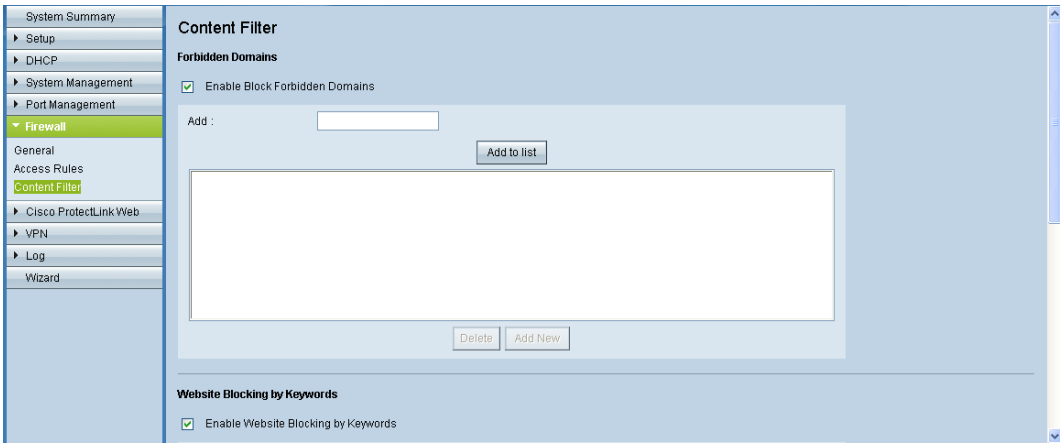
Dans la fenêtre *Service Management*, ajoutez ou mettez à jour des entrées, selon vos besoins. Avant de fermer cette fenêtre, cliquez sur **OK** pour enregistrer vos paramètres ou sur **Cancel** pour les annuler. Les modifications non enregistrées ne sont pas prises en compte.

- **Pour ajouter un service à la liste:** saisissez les informations suivantes, puis cliquez sur **Add to list**. La liste peut comporter jusqu'à 30services.
  - **Service Name :** entrez une brève description.
  - **Protocol :** sélectionnez le protocole requis. Reportez-vous à la documentation du service que vous hébergez.
  - **Port Range :** saisissez la plage de ports requise.
- **Pour ajouter un nouveau service:** saisissez les informations, puis cliquez sur **Add to list**.
- **Pour modifier un service que vous avez créé:** cliquez sur le service dans la liste. Les informations apparaissent dans les champs de texte. Apportez les modifications voulues, puis cliquez sur **Update**. Si aucune modification n'est nécessaire, vous pouvez cliquer sur **Add New** pour annuler la sélection du service et vider les champs de texte.
- **Pour supprimer un service de la liste:** cliquez sur l'entrée à supprimer. Pour sélectionner un bloc d'entrées, cliquez sur la première entrée, maintenez la touche **Maj** enfoncée, puis cliquez sur la dernière entrée du bloc. Pour sélectionner plusieurs entrées individuelles, maintenez la touche **Ctrl** enfoncée tout en cliquant sur les entrées. Cliquez sur **Delete**.

Utilisation de filtres de contenu pour contrôler l'accès à Internet

Utilisez la page *Firewall> Content Filter* pour empêcher les utilisateurs d'accéder à des sites Web inappropriés. Vous pouvez bloquer l'accès en spécifiant des domaines et des mots clés.

Pour ouvrir cette page: Cliquez sur **Firewall> Content Filter** dans l'arborescence.



REMARQUE Avant de quitter cette page, cliquez sur **Save** pour enregistrer vos paramètres ou sur **Cancel** pour les annuler. Les modifications non enregistrées ne sont pas prises en compte.

Vous pouvez bloquer l'accès à des domaines spécifiés, bloquer une série de sites plus vaste ou encore bloquer l'accès à des adresses URL contenant des mots clés spécifiques. Vous pouvez également spécifier les jours et les heures d'activation de ces filtres. Cette page comprend les sections suivantes:

- **Forbidden Domains, page 115**
- **Website Blocking by Keywords, page 115**
- **Schedule, page 116**

REMARQUE Les règles de filtrage de contenu sont automatiquement désactivées si le service Cisco ProtectLink est activé sur le routeur. Configurez plutôt les fonctionnalités ProtectLink pour contrôler l'accès à Internet. Pour plus d'informations, reportez-vous au **Chapitre 8, « Cisco ProtectLink Web ».**

Forbidden Domains

Cochez la case **Enable Block Forbidden Domains** pour permettre au routeur de bloquer l'accès aux domaines spécifiés. Décochez la case pour désactiver cette option.

Ajoutez ou modifiez des règles, selon les besoins. Notez que vos entrées ne sont pas enregistrées tant que vous n'avez pas cliqué sur le bouton Save.

- **Pour ajouter une entrée à la liste:** saisissez le nom de domaine dans le champ **Add**, puis cliquez sur **Add to list**. Répétez cette tâche autant de fois que nécessaire pour ajouter d'autres domaines.

  L'accès est bloqué si un utilisateur saisit un nom de domaine spécifié dans la barre d'adresse du navigateur ou s'il accède à une page Web située au sein d'un domaine spécifié. Imaginons, par exemple, que le site *yahoo.com* soit bloqué. L'utilisateur ne peut saisir aucune adresse URL commençant par *yahoo.com*. L'accès est également bloqué si l'utilisateur effectue une recherche sur Internet et clique sur un lien vers une page située dans le domaine spécifié, comme *yahoo.com/news*. Toutefois, l'utilisateur peut se connecter au site *mail.yahoo.com*, qui correspond à un domaine différent.

- **Pour modifier une entrée de la liste:** cliquez sur l'entrée à modifier. Apportez les modifications voulues, puis cliquez sur **Update**. Si aucune modification n'est nécessaire, vous pouvez cliquer sur **Add New** pour annuler la sélection de l'entrée et vider le champ de texte.

- **Pour supprimer une entrée de la liste:** cliquez sur l'entrée à supprimer, puis cliquez sur **Delete**.

Website Blocking by Keywords

Cochez la case **Enable Website Blocking By Keywords** pour permettre au routeur de bloquer l'accès à des adresses URL comportant des caractères spécifiques. Décochez la case pour désactiver cette option.

Ajoutez ou modifiez des règles, selon les besoins. Notez que vos entrées ne sont pas enregistrées tant que vous n'avez pas cliqué sur le bouton Save.

- **Pour ajouter une entrée à la liste:** saisissez le mot-clé dans le champ **Add**, puis cliquez sur **Add to list**. Un mot clé peut correspondre à un mot complet, comme *gouvernement* ou à quelques caractères uniquement, comme *gouv*. Répétez cette tâche autant de fois que nécessaire, pour ajouter d'autres mots clés.

L'accès est bloqué si l'utilisateur saisit une adresse URL comportant les caractères spécifiés ou s'il accède à une telle adresse. Imaginons, par exemple, que le terme *yahoo* soit bloqué. L'utilisateur ne peut pas accéder aux sites suivants: *www.yahoo.com*, *finance.yahoo.com* et *mydomain.com/news/yahoo*.

- **Pour modifier une entrée de la liste:** cliquez sur l'entrée à modifier. Apportez les modifications voulues, puis cliquez sur **Update**. Si aucune modification n'est nécessaire, vous pouvez cliquer sur **Add New** pour annuler la sélection de l'entrée et vider le champ de texte.
- **Pour supprimer une entrée de la liste:** cliquez sur l'entrée à supprimer, puis cliquez sur **Delete**.

Schedule

Conservez les paramètres par défaut ou programmez la période d'activation du filtrage de contenu:

- **Time:** sélectionnez l'une des options suivantes:
  - **Always :** sélectionnez cette option si la règle s'applique tout le temps, tous les jours de la semaine. Vous pouvez éventuellement saisir une période dans les champs *From* et *To*.
  - **Interval :** sélectionnez cette option pour spécifier la période pendant laquelle la règle est active. Si vous choisissez cette option, vous devez saisir une période dans les champs *From* et *To*. Vous pouvez éventuellement spécifier les jours de la semaine.
- **From** et **To :** si vous choisissez Interval, utilisez ces champs pour spécifier les heures et les jours d'activation de la règle. Saisissez l'heure de début dans le champ From et l'heure de fin dans le champ To. Utilisez le format hh:mm (15:30 correspond à 15h30). Saisissez 00:00 à 00:00 si la règle s'applique à toutes les heures du jour.
- **Effective on :** si vous choisissez Interval, utilisez ces cases pour spécifier les jours pendant lesquels la règle est active. Cochez la case **Everyday** si la règle est active tous les jours. Pour sélectionner des jours spécifiques, décochez la case **Everyday**, puis activez la case correspondant à chaque jour d'activation de la règle.

8

Cisco ProtectLink Web

Le service facultatif Cisco ProtectLink Web permet de sécuriser votre réseau. Ce service est disponible pour tous les routeurs de la gamme RV0xx à l'exception de CiscoRV042G. Cisco ProtectLink Web filtre les adresses de site Web (URL) et bloque les sites Web potentiellement malveillants. Reportez-vous aux rubriques suivantes:

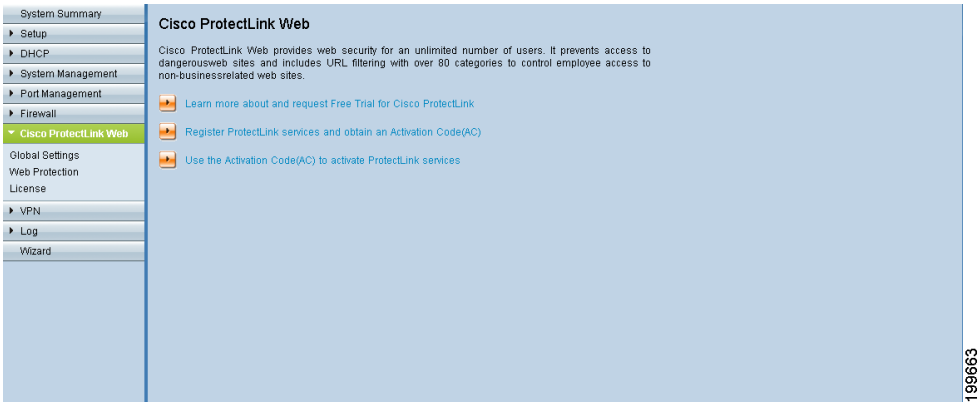
- **Mise en route de CiscoProtectLink Web, page 117**
- **Spécification des paramètres globaux des URL et des clients homologués, page 119**
- **Mise à jour de la licence ProtectLink, page 124**

REMARQUE Pour obtenir plus d'informations sur ce produit Cisco, allez à la page d'informations sur le service Cisco ProtectLink Web, à l'adresse www.cisco.com/en/US/products/ps9953/index.html

Mise en route de CiscoProtectLink Web

Vous pouvez acheter, enregistrer et activer le service à l'aide des liens de la page *Cisco ProtectLink Web*.

Pour ouvrir cette page: cliquez sur **Cisco ProtectLink Web** dans l'arborescence.



Choisissez l'option appropriée:

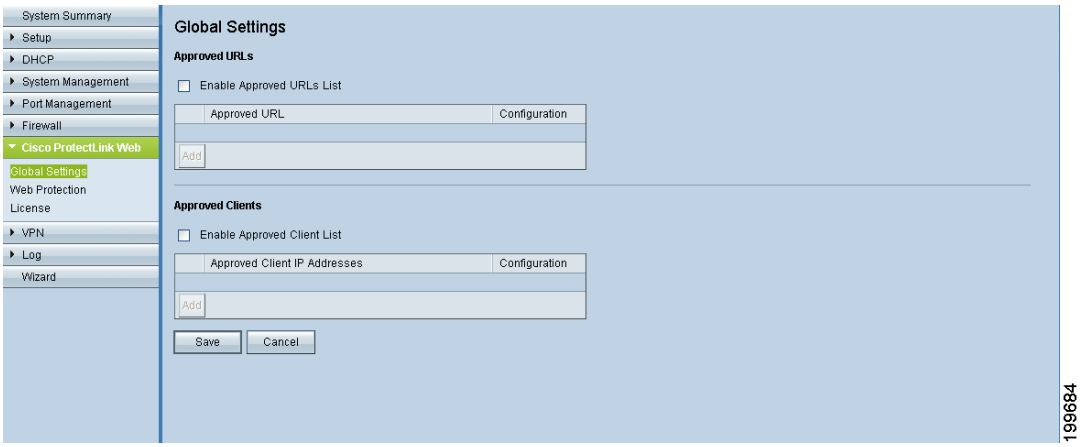
- **Learn more about and request Free Trial for Cisco ProtectLink:** cliquez sur ce lien pour ouvrir la page Cisco ProtectLink Security Solutions du site Cisco.com. Vous pouvez lire les informations sur le produit et bénéficier d'une période d'essai de 30jours pour votre routeur RV.
- **Register ProtectLink services and obtain an Activation Code (AC):** cliquez sur ce lien si vous avez acheté le produit et êtes prêt à l'enregistrer. Lorsque la page d'enregistrement apparaît, suivez les instructions affichées à l'écran pour saisir votre clé d'enregistrement et renseigner les informations requises. Fermez la page Web lorsque vous avez terminé. Le code d'activation s'affiche à l'écran et est envoyé à l'adresse e-mail que vous avez fournie.
- **Use the Activation Code (AC) to activate ProtectLink services:** cliquez sur ce lien si, après avoir enregistré le produit, vous avez reçu un code d'activation. Lorsque la page d'activation apparaît, saisissez votre code d'activation et suivez les instructions affichées à l'écran. Fermez la page Web lorsque vous avez terminé. Actualisez le navigateur Web: les fonctionnalités de ProtectLink Web sont dorénavant disponibles sur votre routeur. La page *Global Settings* s'affiche.

REMARQUE Si vous remplacez un routeur par un autre routeur qui prend en charge ce service, vous pouvez utiliser le lien **Use the Activation Code** pour transférer votre licence d'utilisation du service ProtectLink vers le nouveau routeur.

Spécification des paramètres globaux des URL et des clients homologués

Après avoir activé le service, vous pouvez utiliser la page *Cisco ProtectLink Web > Global Settings* pour configurer les services sur le routeur.

Pour ouvrir cette page: cliquez sur **ProtectLink> Global Settings** dans l'arborescence.



REMARQUE Cette page n'est disponible que si vous avez activé le service Cisco ProtectLink Web. Reportez-vous à **Mise en route de CiscoProtectLink Web, page 117**.

Vous pouvez spécifier les URL auxquelles les utilisateurs peuvent accéder à tout moment. Vous pouvez également spécifier les clients homologués qui ne sont pas soumis aux restrictions que vous configurez dans la protection Web.

Pour ajouter une entrée dans le tableau *Approved URLs* ou *Approved Clients*, cliquez sur **Add**. Pour supprimer une entrée, cliquez sur l'icône Delete.

REMARQUE Avant de quitter cette page, cliquez sur **Save** pour enregistrer les paramètres ou sur **Cancel** pour les annuler. Les modifications non enregistrées ne sont pas prises en compte.

URL approuvées et clients homologués

Après avoir cliqué sur le bouton Add à la page *Cisco ProtectLink Web> Global Settings*, la page Configuration s'affiche.

REMARQUE Avant de quitter cette page, cliquez sur **Save** pour enregistrer les paramètres ou sur **Cancel** pour les annuler. Les modifications non enregistrées ne sont pas prises en compte.

Approved URL Configuration

Les domaines qui figurent sur cette liste sont toujours accessibles, quels que soient les paramètres de protection Web.

Cochez la case **Enable Approved URL List** pour activer cette fonctionnalité. Vous pouvez ensuite ajouter jusqu'à 20 URL homologuées et toujours accessibles.

- **Pour ajouter des entrées:** cliquez sur **Add New** pour ouvrir la page *Approved URL Configuration*. Saisissez la (les) URL homologuée(s) dans la zone de texte. Pour saisir plusieurs URL, insérez un point-virgule entre les entrées, comme suit: *www.cisco.com;www.google.com; www.monentreprise.com*. Toutes les pages des domaines spécifiés seront accessibles. Cliquez sur **Save** pour enregistrer vos modifications ou sur **Cancel** pour les annuler.

  Si vous avez saisi des caractères non valides, un message s'affiche. Cliquez sur **OK** pour fermer le message et modifiez vos entrées. Les espaces, les virgules et les symboles ne sont pas autorisés.

- **Pour supprimer une entrée:** cliquez sur l'icône **Delete**.

Approved Clients Configuration

Les clients figurant sur cette liste peuvent toujours se connecter à tous les sites Web. La protection Web n'interdit pas les requêtes d'URL provenant de ces adresses IP.

Cochez la case **Enable Approved Client List** pour activer cette fonctionnalité. Vous pouvez ensuite ajouter jusqu'à 20clients homologués (adresses IP locales) qui pourront toujours accéder aux URL filtrées.

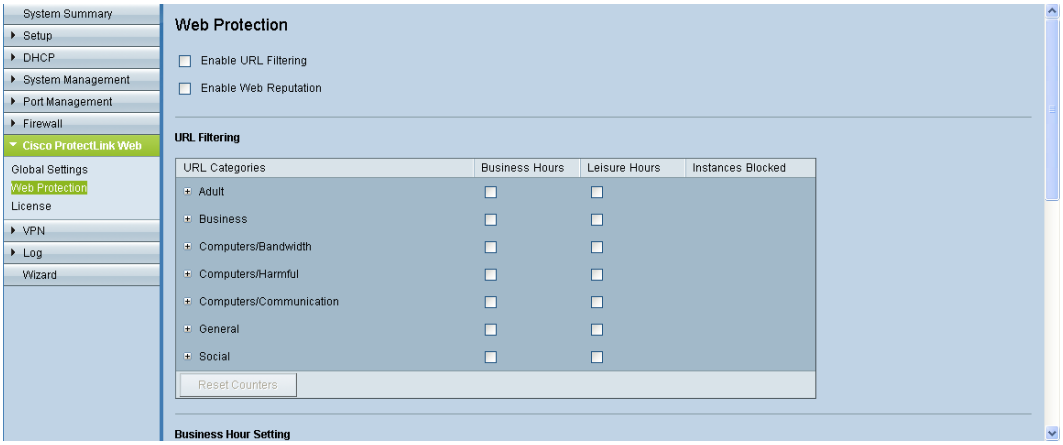
- **Pour ajouter des entrées:** saisissez des adresses IP ou des plages d'adresses IP. Pour saisir des adresses IP non consécutives, insérez un point-virgule entre les entrées, comme suit: *10.1.1.1;10.1.1.5*. Pour saisir une plage d'adresses IP, insérez un trait d'union entre la première adresse et la dernière adresse de la plage, comme suit: *10.1.1.0-10.1.1.10*.

- **Pour supprimer une entrée:** cliquez sur l'icône **Delete**.

Activation de la protection Web pour le filtrage des URL

Utilisez la page *Cisco ProtectLink Web> Web Protection* pour configurer le filtrage des URL et les paramètres de réputation Web.

Pour ouvrir cette page: cliquez sur **ProtectLink> Web Protection** dans l'arborescence.



REMARQUE

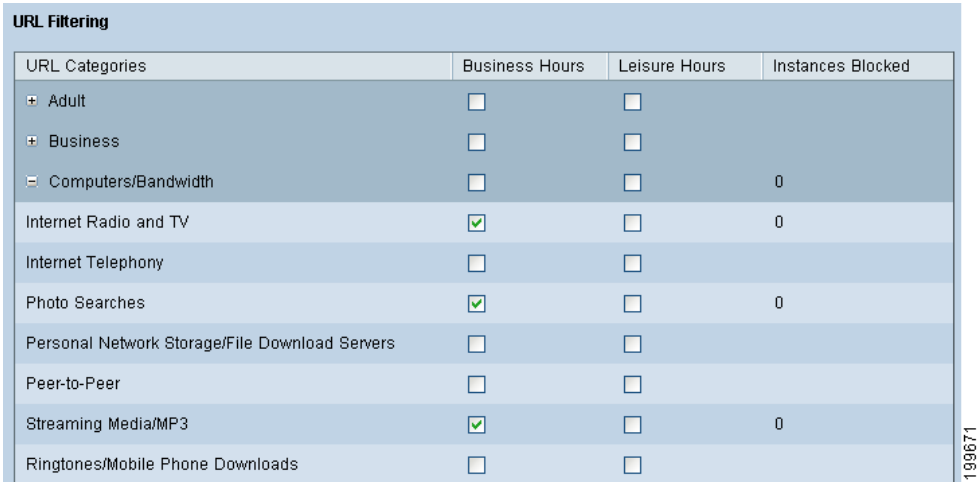
- Cette page n'est disponible que si vous avez activé le service Cisco ProtectLink Web. Reportez-vous à **Mise en route de CiscoProtectLink Web, page 117**.
- Avant de quitter cette page, cliquez sur **Save** pour enregistrer les paramètres ou sur **Cancel** pour les annuler. Les modifications non enregistrées ne sont pas prises en compte.

Web Protection

- **Enable URL Filtering:** cochez cette case pour bloquer l'accès aux sites Web qui appartiennent à des catégories prédéfinies. Désactivez la case pour désactiver ce service.
- **Enable Web Reputation:** cochez cette case pour comparer les requêtes d'URL aux entrées de la base de données de sécurité de Cisco ProtectLink Web. Ce service est recommandé pour bloquer les sites Web potentiellement malveillants. Décochez la case pour désactiver ce service.

URL Filtering

Sélectionnez les catégories et sous-catégories des sites Web auxquels vous souhaitez bloquer l'accès pendant les heures ouvrées et pendant les heures de fermeture.



REMARQUE Pour définir les heures ouvrées et les heures de fermeture, reportez-vous à la section *Business Hour Setting*. Si vous conservez les paramètres par défaut des heures ouvrées, tous les jours et toutes les heures sont classés dans la catégorie Business Hours. Vous pouvez ignorer les cases à cocher Leisure Hours.

- Pour afficher les sous-catégories d'une catégorie donnée, cliquez sur le signe plus(+).
- Pour bloquer l'accès à toutes les sous-catégories d'une catégorie donnée, cochez la case qui correspond à cette catégorie. Pour désactiver le filtrage d'une catégorie donnée, décochez la case.
- Pour bloquer l'accès à des sous-catégories individuelles, cochez les cases individuelles. Pour désactiver le filtrage d'une sous-catégorie donnée, décochez chaque case.
- **Instances Blocked:** pour chaque filtre activé, le nombre de tentatives d'accès à un site bloqué est affiché dans la colonne.
- **Reset Counters:** le routeur compte le nombre de tentatives d'accès à une URL interdite. Pour remettre le compteur à zéro, cliquez sur le bouton.

Business Hour Setting

Utilisez les paramètres de cette section pour définir les heures ouvrées et les heures de fermeture du filtrage des URL.

REMARQUE Si vous conservez les paramètres par défaut des heures ouvrées, tous les jours et toutes les heures sont classés dans la catégorie Business Hours. Si vous sélectionnez des jours et des heures spécifiques, les périodes sélectionnées sont des heures ouvrées et les périodes non sélectionnées, des heures de fermeture.

- **Business Days:** cochez cette case pour chaque jour ouvré dans votre entreprise. Décochez la case pour chaque jour de fermeture de votre entreprise. Les filtres d'heures ouvrées sont appliqués les jours sélectionnés. Les filtres d'heures de fermeture sont appliqués les jours non sélectionnés.
- **Business Times:** pour utiliser les mêmes paramètres tout au long de la journée, conservez le paramètre par défaut, **All day (24hours)**. Pour spécifier les heures d'ouverture de votre entreprise, cliquez sur **Specify business hours**. Cochez la case **Morning** et sélectionnez l'heure de début (*From* et de fin (*To*). Cochez ensuite la case **Afternoon** et sélectionnez l'heure de début (*From*) et de fin (*To*). Pendant les périodes sélectionnées, les filtres des heures ouvrées sont appliqués. Pendant toutes les autres périodes, les filtres des heures de fermeture sont appliqués.

Web Reputation

Sélectionnez le niveau de sécurité adéquat:

- **High:** cette option bloque un nombre élevé de sites Web potentiellement malveillants, mais génère également un taux plus important de faux positifs (sites légitimes classifiés comme étant malveillants).
- **Medium:** cette option bloque la plupart des sites Web potentiellement malveillants et génère un taux moins important de faux positifs (sites légitimes classifiés comme étant malveillants). **Medium** est le paramètre recommandé.
- **Low:** cette option bloque moins de sites Web potentiellement malveillants, ce qui réduit le risque de faux positifs.

URL Overflow Control

Spécifiez le comportement à adopter par ce service pendant les périodes où le nombre de requêtes d'URL dépasse la capacité de gestion du service.

- **Temporarily block URL requests:** ce paramètre est recommandé. Sélectionnez cette option pour contenir le dépassement de capacité jusqu'à ce que les requêtes puissent être traitées. Il s'agit du paramètre par défaut.
- **Temporarily bypass URL verification for requested URLs:** sélectionnez cette option pour permettre que toutes les requêtes en excédent soient transférées sans vérification. Ce paramètre n'est pas recommandé.

Mise à jour de la licence ProtectLink

Utilisez la page *Cisco ProtectLink Web> License* pour afficher les informations sur votre licence ou pour renouveler cette dernière.

Pour ouvrir cette page: cliquez sur **ProtectLink> License** dans l'arborescence.

REMARQUE Cette page n'est disponible que si vous avez activé le service Cisco ProtectLink Web. Reportez-vous à **Mise en route de CiscoProtectLink Web, page 117**.

License

- **Update Information:** pour actualiser les informations sur la licence affichées à l'écran, cliquez sur **Update Information**.

License Information

- **View detailed license online:** pour consulter les informations sur la licence, cliquez sur ce lien. Votre navigateur Web ouvre la page *ProtectLink Product Detail*. Vous pouvez fermer cette page après avoir lu les informations.
- **Status:** état de votre licence: *Activated* ou *Expired*.
- **Platform:** type de plate-forme, Gateway Service.
- **License expires on:** date et heure auxquelles votre licence expire (un an après l'activation du service).
- **Renew:** pour obtenir des informations sur le renouvellement de votre licence, cliquez sur **Renew**. Après avoir acheté une clé d'extension, vous pouvez l'enregistrer et activer le service.

9

VPN

Utilisez le module VPN pour configurer un VPN (Virtual Private Network, réseau privé virtuel) afin de créer un accès sécurisé à votre site, depuis des emplacements distants. Reportez-vous aux rubriques suivantes:

Présentation du protocole VPN

Un VPN (réseau privé virtuel) est une connexion entre deux points de terminaison situés dans différents réseaux, qui permet l'envoi sécurisé de données privées sur un réseau partagé ou public, comme Internet, par exemple. Ce tunnel permet de créer un réseau privé capable d'envoyer des données de manière sécurisée entre ces deux emplacements ou réseaux. Les tunnels VPN utilisent des techniques d'authentification et de cryptage standard, afin de sécuriser les données envoyées entre les deux réseaux. Il peut permettre de créer des liaisons réseau sécurisées entre un bureau central et ses filiales, ses télétravailleurs et/ou ses travailleurs mobiles.

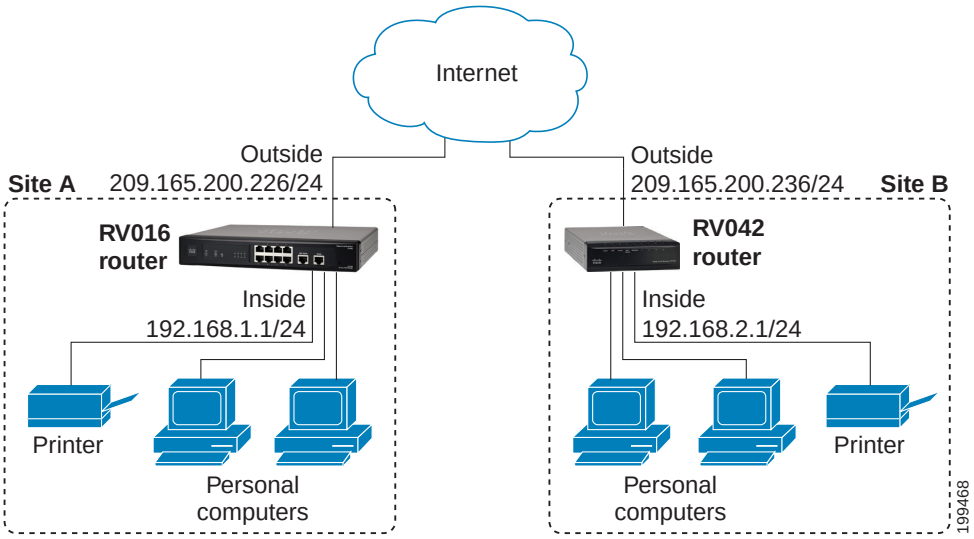
Il existe plusieurs façons de créer une connexionVPN:

- **Accès à distance avec Cisco QuickVPN, page 129**
- **Accès à distance avec PPTP, page 129**

VPN de site à site (passerelle à passerelle)

Dans un VPN de site à site ou de passerelle à passerelle, un routeur VPN situé dans un bureau se connecte à un routeur VPN situé dans un bureau distant. Les périphérique client ont accès aux ressources réseau comme s'ils se trouvaient tous sur le même site. Ce modèle peut servir à plusieurs utilisateurs situés dans un bureau distant.

Dans l'exemple suivant, le bureau central (site A) et un bureau distant (site B) sont reliés par un tunnel VPN. Les utilisateurs des deux sites ont accès aux ressources réseau sur les deux sites.



Tâches de configuration :

Utilisez la page *VPN > Gateway to Gateway* pour configurer le tunnel VPN. Pour obtenir des instructions, reportez-vous à la section **Configuration d'un VPN inter-passerelle (inter-site), page 134**. Pour obtenir plus d'informations et d'exemples, reportez-vous à **Annexe D, « Configuration d'un tunnel VPN passerelle à passerelle connecté entre deux routeurs de la gamme RV0xx. »**..

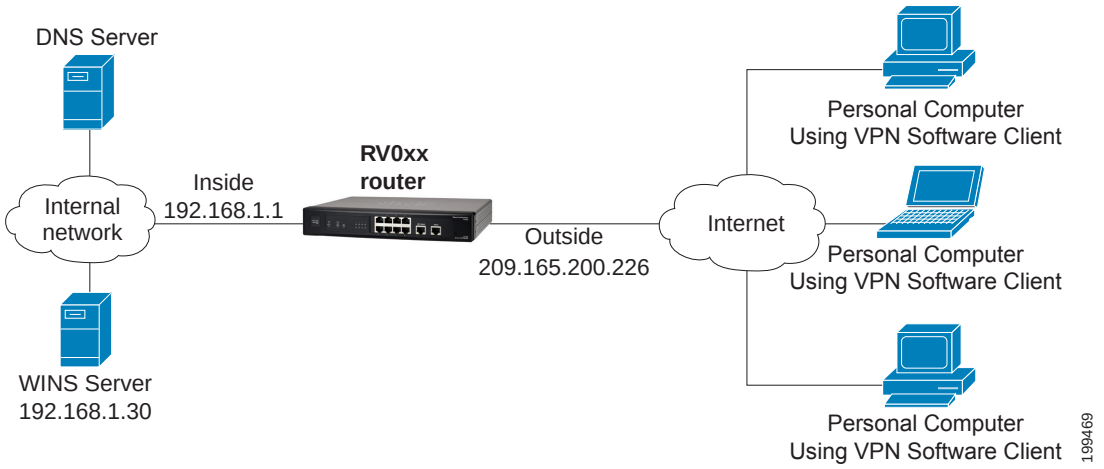
Accès distant (client à passerelle)

Lors d'un accès distant ou avec un tunnel Client vers Passerelle, un ordinateur avec logiciel client VPN se connecte à un routeur VPN. Dans ce premier scénario, vous pouvez installer un logiciel client VPN tiers sur les ordinateurs des utilisateurs. Si vous choisissez de ne pas recourir au logiciel client VPN, tout ordinateur équipé du gestionnaire de sécurité IPSec intégré (Windows 2000, Windows XP et Windows 7) accède à un tunnel VPN.

Vous devrez configurer ce routeur selon les stratégies IPsec requises par le client IPsec. Vous serez également amené à installer et configurer le logiciel client IPsec sur les ordinateurs des utilisateurs.

REMARQUE Examinez deux autres options d'accès à distance: **Accès à distance avec Cisco QuickVPN, page 129** et **Accès à distance avec PPTP, page 129**.

La figure suivante est un exemple de VPN établi entre un client et une passerelle. Un employé en déplacement se connecte à Internet à partir de sa chambre d'hôtel. Sur son ordinateur portable, le logiciel clientVPN est configuré avec les paramètresVPN de son bureau. L'utilisateur accède au logiciel client VPN et se connecte au routeur VPN du bureau central. Grâce au VPN, cette personne dispose d'une connexion sécurisée au réseau du site central de sa société, comme si elle y était physiquement connectée.



Tâches de configuration :

1. Utilisez la page *VPN > Client to Gateway* pour configurer le tunnel VPN avec les paramètres requis par le client tiers tel que TheGreenbow. Pour obtenir des instructions, reportez-vous à la section **Configuration d'un tunnel d'accès à distance pour les clients VPN (client à passerelle), page 144**.
2. Installez le logiciel client sur les ordinateurs des utilisateurs.

Accès à distance avec Cisco QuickVPN

Les utilisateurs disposant du logiciel Cisco QuickVPN peuvent établir un tunnel VPN sur votre réseau. Recourez à cette option si vous désirez simplifier le processus de configuration VPN. Il est inutile de configurer des stratégies VPN. Les utilisateurs distants peuvent se connecter en toute sécurité grâce au client Cisco QuickVPN et une connexion Internet. Pour plus d'informations sur les avantages et les limites, voir « Easy and Secure Access with Cisco QuickVPN » à l'adresse http://www.cisco.com/en/US/docs/routers/csbr/app_notes/QuickVPN_an_OL-25680.pdf

Tâches de configuration :

1. Utilisez la page *VPN Client Access* page pour ajouter des noms d'utilisateurs et des mots de passe.
2. Vous pouvez aussi utiliser la page *VPN > VPN Client Access* pour générer des certificats à installer sur les ordinateurs des utilisateurs. Pour plus d'informations, voir **Certificate Management, page 156**.
3. Installez Cisco QuickVPN sur les ordinateurs des utilisateurs. Pour vous procurer le logiciel, rendez-vous sur www.cisco.com/go/software. Saisissez le numéro de modèle du routeur dans la zone de recherche, puis cliquez sur **Find**. Dans la liste des liens, cliquez sur **Quick Virtual Private Network (QVPN) Utility**. Après avoir téléchargé le logiciel sur l'ordinateur, double-cliquez sur **Setup.exe** pour lancer l'installation.
4. Si vous avez généré des certificats, copiez le certificat vers le répertoire dans lequel Cisco QuickVPN est installé, en général dans C:\Program Files\Cisco Small Business\QuickVPN client.

Accès à distance avec PPTP

Un utilisateur distant équipé d'un ordinateur Microsoft peut établir un tunnel VPN en se connectant à un serveur PPTP à niveau de votre site. Cette option permet de simplifier la configuration VPN. Il est inutile de configurer les stratégies VPN sur le routeur et d'installer un client VPN sur les ordinateurs des utilisateurs. Toutefois, rappelez-vous que des vulnérabilités de sécurité ont été trouvées dans ce protocole.

Tâches de configuration :

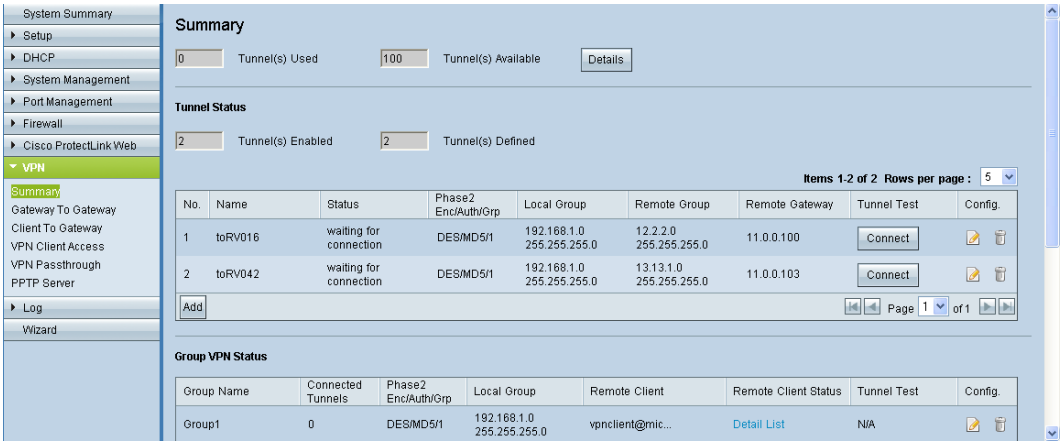
1. Utilisez la page *VPN > PPTP Server* pour activer le serveur PPTP, définir la plage d'adressesIP pour les clients et saisir les noms d'utilisateurs et les mots de passe.
2. Distribuez les noms d'utilisateurs et les mots de passe aux utilisateurs.

Consultation des informations générales des VPN

La page *VPN > Summary* affiche des informations générales relatives aux paramètres des tunnels VPN du routeur. Le routeur prend en charge jusqu'à 100tunnels.

REMARQUE Si le serveur PPTP est activé, les informations générales relatives aux clients PPTP s'affichent sur la page *VPN > PPTP Server*. Pour plus d'informations, voir **Configuration d'un serveur PPTP, page 158**.

Pour ouvrir cette page : cliquez sur **VPN > Summary** dans l'arborescence.



Résumé

- **Tunnel(s) Used:** nombre de tunnels VPN utilisés.
- **Tunnels Available:** nombre de tunnels VPN disponibles.
- **Detail:** cliquez sur **Detail** pour de plus amples renseignements. Cliquez sur **Refresh** pour mettre à jour les données ou sur **Close**, pour revenir à la page *VPN > Summary*. Les paramètres No., Name, Status, Phase 2 Enc/Auth/Grp, Local Group, Remote Group et Remote Gateway de chaque tunnel VPN s'affichent.

Tunnel Status

Les informations suivantes sont affichées au-dessus du tableau:

- **Tunnel(s) Enabled:** nombre de tunnels activés.
- **Tunnel(s) Defined:** nombre de tunnels définis, qu'ils soient activés ou non.

Le tableau répertorie les informations suivantes, pour chaque tunnel:

- **No.:** numéro d'identification du tunnel VPN.
- **Name:** nom descriptif du tunnel VPN.
- **Status:** état du tunnel VPN: *Connected* ou *Waiting for Connection*.
- **Phase2 Enc/Auth/Grp:** Le type de cryptage de phase2 (NULL/DES/3DES/AES-128/AES-192/AES-256), méthode d'authentification (NULL/MD5/SHA1) et numéro de groupe DH (02/01/05) choisis dans la section IPSec Setup.

  Si vous avez réglé le paramètre Keying Mode sur Manual, dans la section IPSec, seuls le type de cryptage et la méthode d'authentification s'affichent.
- **Local Group:** adresse IP et masque de sous-réseau du groupe local.
- **Remote Group:** adresse IP et masque de sous-réseau du groupe distant.
- **Remote Gateway:** adresseIP de la passerelle distante.
- **Tunnel Test:** cliquez sur **Connect** pour consulter l'état du tunnel VPN. Le résultat du test est alors mis à jour dans la colonne *Status*. Si le tunnel est connecté, un bouton Disconnect apparaît, afin de vous permettre de mettre fin à la connexion.
- **Configure:** cliquez sur l'icône **Edit** pour ouvrir une nouvelle page permettant de modifier les paramètres du tunnel. Pour supprimer les paramètres d'un tunnel, sélectionnez-le et cliquez sur l'icône **Delete**.
- **Tunnel Enabled:** nombre de tunnels VPN activés.
- **Tunnel Defined:** nombre de tunnels VPN définis.
- **Add:** cliquez sur ce bouton pour ajouter un tunnel. Choisissez ensuite l'une des options suivantes:
  - Pour créer un tunnel destiné à un site distant équipé d'un routeur VPN, choisissez **Gateway to Gateway**. La page *Gateway to Gateway* s'affiche. Reportez-vous à **Configuration d'un VPN inter-passerelle (inter-site), page 134**.

- Pour créer un tunnel destiné à un travailleur distant, à l'aide d'un logiciel client VPN, choisissez **Client to Gateway**. La page *Client to Gateway* s'affiche. Reportez-vous à **Configuration d'un tunnel d'accès à distance pour les clients VPN (client à passerelle), page 144**.

- **Navigation controls:** si vous disposez de nombreuses règles, vous pouvez ajuster l'affichage. Utilisez l'option *Rows per page list*, située dans le coin supérieur droit du tableau, pour choisir le nombre de règles à afficher sur chaque page. Utilisez la liste *Page*, située au-dessous du tableau, pour choisir une page spécifique. Utilisez les boutons de navigation pour afficher la première page, la page précédente, la page suivante ou la dernière page. Selon le nombre de pages dont vous disposez et la sélection actuelle, certains boutons risquent de ne pas être disponibles.

GroupVPN Status

Si vous activez le paramètre GroupVPN pour un de vos tunnels Client to Gateway, les informations relatives à l'état apparaissent dans ce tableau.

- **Group Name:** nom descriptif du VPN de groupe.
- **Connected Tunnels:** nombre d'utilisateurs connectés au VPN de groupe.
- **Phase2 Enc/Auth/Grp:** Le type de cryptage de phase2 (NULL/DES/3DES/AES-128/AES-192/AES-256), méthode d'authentification (NULL/MD5/SHA1) et numéro de groupe DH (02/01/05) choisis dans la section *IPSec Setup*.
- **Local Group:** adresse IP et masque de sous-réseau du groupe local.
- **Remote Client:** clients distants du VPN de groupe.
- **Remote Clients Status:** état des clients distants: *Online* ou *Offline*. Cliquez sur **Detail List** pour ouvrir la fenêtre *Group List*. Celle-ci affiche les paramètres Group Name, IP address et Connection Time. Cliquez sur **Refresh** pour mettre à jour les données ou sur **Close** pour fermer la fenêtre contextuelle et revenir à la page *VPN > Summary*.
- **Tunnel Test:** cliquez sur **Connect** pour consulter l'état du VPN de groupe. Le résultat du test est alors mis à jour dans la colonne *Status*. Si le VPN de groupe est connecté, un bouton Disconnect apparaît pour vous permettre de mettre fin à la connexion.
- **Configure:** cliquez sur l'icône **Edit** pour ouvrir une nouvelle page permettant de modifier les paramètres du tunnel. Pour supprimer les paramètres d'un tunnel, sélectionnez-le et cliquez sur l'icône **Delete**.
- **Navigation controls:** si vous disposez de nombreuses règles, vous pouvez ajuster l'affichage. Utilisez l'option *Rows per page list*, située dans le coin

supérieur droit du tableau, pour choisir le nombre de règles à afficher sur chaque page. Utilisez la liste *Page*, située au-dessous du tableau, pour choisir une page spécifique. Utilisez les boutons de navigation pour afficher la première page, la page précédente, la page suivante ou la dernière page. Selon le nombre de pages dont vous disposez et la sélection actuelle, certains boutons risquent de ne pas être disponibles.

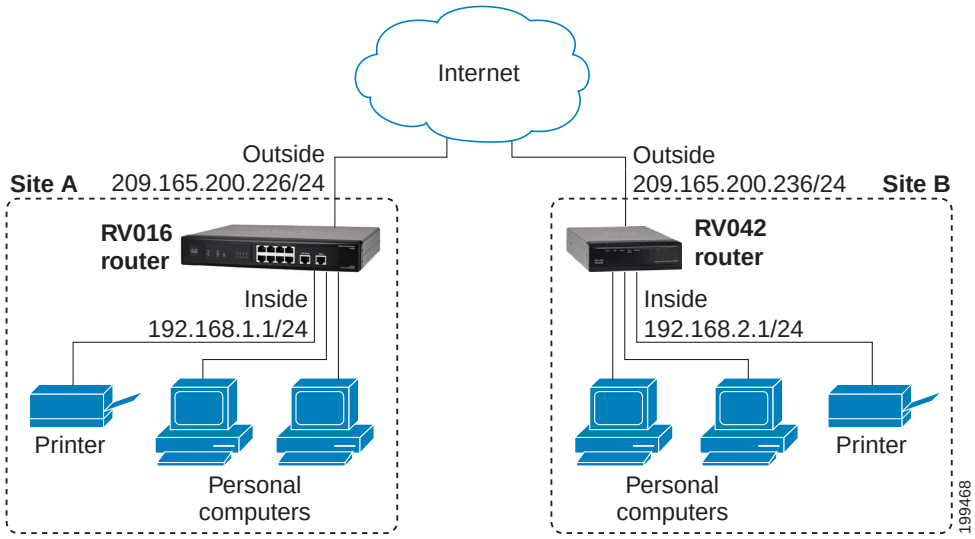
VPN Clients Status

Cette section identifie les clients VPN actuellement connectés au routeur.

- **No.:** numéro d'identification du client VPN.
- **Username:** nom du client VPN.
- **Status:** état de la connexion du client VPN.
- **Start Time:** heure d'établissement de la connexion VPN entre le VPN client et le routeur.
- **End Time:** heure de fin de la connexion VPN entre le VPN client et le routeur.
- **Durée :** durée pendant laquelle la connexion VPN a été active.
- **Disconnect**: cliquez sur ce bouton pour déconnecter un client VPN.
- **Navigation controls:** si vous disposez de nombreuses règles, vous pouvez ajuster l'affichage. Utilisez l'option *Rows per page list*, située dans le coin supérieur droit du tableau, pour choisir le nombre de règles à afficher sur chaque page. Utilisez la liste *Page*, située au-dessous du tableau, pour choisir une page spécifique. Utilisez les boutons de navigation pour afficher la première page, la page précédente, la page suivante ou la dernière page. Selon le nombre de pages dont vous disposez et la sélection actuelle, certains boutons risquent de ne pas être disponibles.

Configuration d'un VPN inter-passerelle (inter-site)

La page *VPN > Gateway to Gateway* vous permet de créer un tunnel entre deux périphériques VPN. Il peut s'agir par exemple d'un routeur CiscoRV082 situé dans votre bureau et d'un routeur CiscoRV042 situé chez un bureau à distance.



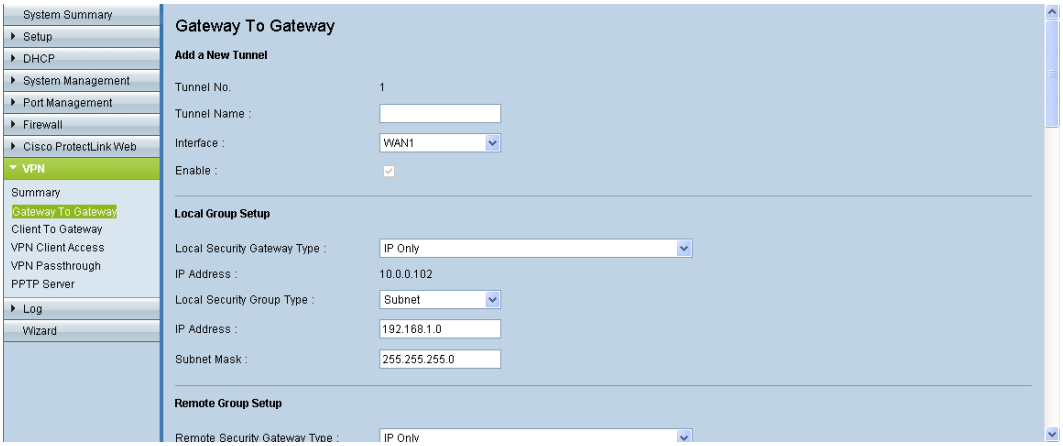
Il vous faudra configurer les paramètres du groupe local et du groupe distant et saisir les paramètres correspondants (en inversant le groupe local et du groupe distant) lors de la configuration de l'autre routeur. Pour établir une connexion, au moins un des routeurs doit être identifiable à l'aide d'une adresse IP statique ou d'un nom d'hôte DNS dynamique. Par ailleurs, si l'un des routeurs possède uniquement une adresse IP dynamique, vous pouvez effectuer l'authentification à l'aide d'une adresse email, afin d'établir la connexion.

REMARQUE Les deux extrémités du tunnel ne doivent pas se trouver sur le même sous-réseau. Si, par exemple, le site A LAN utilise le masque de sous-réseau 192.168.1.x, le site B peut utiliser le masque 192.168.2.x.

Vous saisissez les paramètres correspondants (en inversant le groupe local et le groupe distant) lors de la configuration des deux routeurs. Lors de la configuration de ce routeur (RouteurA), saisissez ses paramètres dans la section *Local Group Setup* et saisissez les paramètres de l'autre routeur (RouteurB) dans la section *Remote Group Setup*. Lors de la configuration de l'autre routeur (RouteurB), saisissez ses paramètres dans la section *Local Group Setup* et saisissez les

paramètres du RouteurA dans la section *Remote Group Setup*. Pour obtenir plus d'informations et d'exemples, reportez-vous à l'**Annexe D, « Configuration d'un tunnel VPN passerelle à passerelle connecté entre deux routeurs de la gamme RV0xx. »**..

Pour ouvrir cette page: cliquez sur **VPN> Gateway to Gateway** dans l'arborescence. Vous pouvez également cliquer sur le bouton **Add Tunnel** de la section *Tunnel Status*, sur la page *VPN > Summary*. Choisissez ensuite **Gateway to Gateway**.



REMARQUE Avant de quitter cette page, cliquez sur **Save** pour enregistrer vos paramètres ou sur **Cancel** pour les annuler. Les modifications non enregistrées ne sont pas prises en compte.

Add a New Tunnel

- **Tunnel No:** numéro d'identification généré automatiquement.
- **Tunnel Name:** saisissez le nom de ce tunnel VPN: Bureau de Paris, Succursale de Lyon ou Service de Bordeaux, par exemple. La description vous sert de référence. Il n'est pas nécessaire qu'elle corresponde au nom utilisé à l'autre extrémité du tunnel.
- **Interface:** choisissez le port WAN à utiliser pour ce tunnel.
- **Enable:** cochez ou décochez cette case pour activer ou désactiver le tunnel VPN. Par défaut, le tunnel est activé.

Local Group Setup et Remote Group Setup

Saisissez les paramètres décrits ci-après. Les paramètres Local correspondent à ceux de ce routeur et les paramètres Remote correspondent à ceux du routeur situé à l'autre extrémité du tunnel. Reproduisez ces paramètres, lors de la configuration du tunnel VPN sur l'autre routeur.

- **Local/Remote Security Gateway Type:** spécifiez la méthode à utiliser pour identifier le routeur, afin d'établir le tunnel VPN. Le paramètre Local Security Gateway est celui de ce routeur, tandis que le paramètre Remote Security Gateway est celui de l'autre routeur. Au moins un des routeurs doit posséder une adresse IP statique ou un nom d'hôte DNS dynamique, afin d'établir une connexion.
  - **IP Only:** choisissez cette option si ce routeur dispose d'une adresse IP WAN statique. L'adresse IP WAN s'affiche automatiquement.

    S'agissant du paramètre *Remote Security Gateway Type*, un champ supplémentaire apparaît. Si vous connaissez l'adresse IP du routeur VPN distant, choisissez **IP Address**, puis saisissez l'adresse. Si vous ne connaissez pas l'adresse IP du routeur VPN distant, choisissez **IP by DNS Resolved**, puis saisissez le nom de domaine réel du routeur sur Internet. Le routeur CiscoRV082 obtient l'adresse IP du périphérique VPN distant grâce au paramètreIP by DNS Resolved et l'adresseIP du périphérique VPN distant s'affiche ensuite dans la section VPN Status de la page *VPN > Summary*.
  - **IP + Domain Name (FQDN) Authentication:** choisissez cette option si ce routeur dispose d'une adresse IP statique et d'un nom de domaine inscrit. Ce peut être *MonServeur.MonDomaine.com*, par exemple. Saisissez également le paramètre **Domain Name** à utiliser pour l'authentification. Le nom de domaine ne peut être utilisé que pour une seule connexion de tunnel.

    S'agissant du paramètre *Remote Security Gateway Type*, un champ supplémentaire apparaît. Si vous connaissez l'adresse IP du routeur VPN distant, choisissez **IP Address**, puis saisissez l'adresse. Si vous ne connaissez pas l'adresse IP du routeur VPN distant, choisissez **IP by DNS Resolved**, puis saisissez le nom de domaine réel du routeur sur Internet. Le routeur CiscoRV082 obtient l'adresse IP du périphérique VPN distant grâce au paramètreIP by DNS Resolved et l'adresseIP du périphérique VPN distant s'affiche ensuite dans la section VPN Status de la page *VPN > Summary*.

- **IP + E-mail Addr.(USER FQDN) Authentication:** choisissez cette option si ce routeur dispose d'une adresse IP statique et que vous souhaitez utiliser une adresse email pour l'authentification. L'adresse IP WAN actuelle s'affiche automatiquement. Saisissez les adresses email à utiliser pour l'authentification, dans le champ **Email Address**.

  S'agissant du paramètre *Remote Security Gateway Type*, un champ supplémentaire apparaît. Si vous connaissez l'adresse IP du routeur VPN distant, choisissez **IP Address**, puis saisissez l'adresse. Si vous ne connaissez pas l'adresse IP du routeur VPN distant, choisissez **IP by DNS Resolved**, puis saisissez le nom de domaine réel du routeur sur Internet. Le routeur CiscoRV082 obtient l'adresse IP du périphérique VPN distant grâce au paramètreIP by DNS Resolved et l'adresseIP du périphérique VPN distant s'affiche ensuite dans la section VPN Status de la page *VPN > Summary*.

- **Dynamic IP + Domain Name (FQDN) Authentication:** choisissez cette option si ce routeur dispose d'une adresse IP dynamique et d'un nom d'hôte DNS dynamique inscrit (disponible auprès des fournisseurs). Ce peut être DynDNS.com, par exemple. Saisissez le paramètre **Domain Name** à utiliser pour l'authentification. Le nom de domaine ne peut être utilisé que pour une seule connexion de tunnel.

- **Dynamic IP + E-mail Addr.(USER FQDN) Authentication:** choisissez cette option si ce routeur dispose d'une adresse IP dynamique, mais qu'il n'a pas de nom d'hôte DNS dynamique. Saisissez les adresses email à utiliser pour l'authentification, dans le champ **Email Address**.

  Si les deux routeurs disposent d'adresses IP dynamiques (par exemple, dans le cas de connexions PPPoE), ne choisissez pas l'option Dynamic IP + Email Addr. pour les deux passerelles. Pour la passerelle distante, choisissez **IP Address** et **IP Address by DNS Resolved**.

- **Local/Remote Security Group Type:** spécifiez les ressources LAN pouvant utiliser ce tunnel. Le paramètre Local Security Group correspond à celui des ressources LAN de ce routeur, tandis que le paramètre Remote Security Group correspond aux ressources LAN de l'autre routeur.

  - **IP Address:** choisissez cette option pour indiquer le périphérique qu'utilise ce tunnel. Saisissez ensuite l'adresse IP du périphérique.

  - **Subnet:** choisissez cette option (option par défaut) pour autoriser tous les périphériques d'un sous-réseau donné à accéder au tunnel VPN. Saisissez ensuite l'adresse IP de sous-réseau et le masque.

- **IP Range:** choisissez cette option pour indiquer la plage des périphériques que le tunnel VPN peut utiliser. Définissez ensuite la plage d'adresses IP souhaitée. Pour ce faire, saisissez la première adresse de la plage dans le champ **Begin IP** et la dernière adresse de la plage, dans le champ **End IP**.

IPSec Setup

Saisissez les paramètres de sécurité du protocole Internet de ce tunnel.

IMPORTANT : afin de permettre tout cryptage, les deux extrémités du tunnel VPN doivent être configurées avec les mêmes méthodes de cryptage, de décryptage et d'authentification. Saisissez exactement les mêmes paramètres sur les deux routeurs.

- **Keying Mode:** choisissez l'une des méthodes de gestion des clés suivantes:
  - **Manual:** choisissez cette option si vous souhaitez générer vous-même la clé et que vous ne souhaitez pas activer la négociation de clé. La gestion manuelle des clés est utilisée dans les petits environnements statiques ou à des fins de dépannage. Saisissez les paramètres souhaités. Pour obtenir plus d'informations, reportez-vous à la section **Champs obligatoires du mode Manual, page 138**.
  - **IKE with Preshared Key:** choisissez cette option si vous souhaitez utiliser le protocole Internet Key Exchange (IKE) pour configurer une association de sécurité, pour votre tunnel. Le protocole IKE utilise une clé prépartagée pour identifier l'homologue IKE distant. Ce paramètre est recommandé et sélectionné par défaut. Saisissez les paramètres souhaités. Pour obtenir plus d'informations, reportez-vous à la section **Champs obligatoires du mode IKE with Preshared Key, page 139** et à la section **Paramètres avancés du mode IKE with Preshared Key, page 141**.
- **Champs obligatoires du mode Manual**

  Saisissez les paramètres du mode Manual. Veillez à saisir les mêmes paramètres, lors de la configuration de ce tunnel sur l'autre routeur. Les paramètres Incoming / Outgoing SPI doivent être reproduits d'un routeur à l'autre.
  - **Incoming / Outgoing SPI:** l'indice des paramètres de sécurité (SPI) se trouve dans l'en-tête du protocole ESP (Encapsulating Security Payload) et permet au récepteur et à l'émetteur de choisir l'association de sécurité à appliquer au traitement des paquets. Vous pouvez saisir des valeurs hexadécimales comprises entre 100 et ffffffff. Chaque tunnel

doit avoir un SPI entrant et un SPI sortant uniques. Deux tunnels ne peuvent pas partager le même SPI. La valeur du champ Incoming SPI que vous définissez ici doit être identique à la valeur Outgoing SPI définie à l'autre extrémité du tunnel et vice versa.

- **Encryption:** sélectionnez une méthode de cryptage (DES ou 3DES). Ce paramètre détermine la longueur de la clé utilisée pour le cryptage ou le décryptage des paquets ESP. DES correspond à un cryptage 56bits et 3DES, à un cryptage 168bits. 3DES est recommandé, car il est plus sûr.
- **Authentication:** sélectionnez une méthode d'authentification (MD5 ou SHA1). La méthode d'authentification détermine la façon dont les paquets ESP sont validés. MD5 est un algorithme de hachage unidirectionnel qui produit une assimilation128bits. SHA1 est un algorithme de hachage unidirectionnel qui produit une assimilation160bits. SHA1 est recommandé, car il est plus sûr. Assurez-vous que les deux extrémités du tunnel VPN utilisent la même méthode d'authentification.
- **Encryption Key:** saisissez la clé à utiliser pour le cryptage et le décryptage du trafic IP. Si vous avez choisi le cryptage DES, saisissez 16valeurs hexadécimales. Si vous avez choisi le cryptage 3DES, saisissez 40valeurs hexadécimales. Si vous ne saisissez pas suffisamment de valeurs hexadécimales, des zéros seront ajoutés à la clé, afin que celle-ci ait la bonne longueur.
- **Authentication Key:** saisissez la clé à utiliser pour authentifier le trafic IP. Si vous avez choisi l'authentification MD5, saisissez 32valeurs hexadécimales. Si vous avez choisi l'authentification SHA1, saisissez 40valeurs hexadécimales. Si vous ne saisissez pas suffisamment de valeurs hexadécimales, des zéros seront ajoutés à la clé, afin que celle-ci ait la bonne longueur.

▪ **Champs obligatoires du mode IKE with Preshared Key**

Saisissez les paramètres des Phases1 et 2. La phase1 consiste à établir les clés prépartagées, afin de créer un canal de communication authentifié et sécurisé. Lors de la Phase2, les homologues IKE utilisent le canal sécurisé pour négocier les associations de sécurité pour le compte d'autres services, tels qu'IPsec. Veillez à saisir les mêmes paramètres, lors de la configuration de ce tunnel sur l'autre routeur.

- **Phase 1 / Phase 2 DH Group:** DH (Diffie-Hellman) est un protocole d'échange de clés. On distingue trois groupes de longueurs de clés primaires: Group1 - 768bits, Group2 - 1024bits et Group5 - 1536bits. Si vous souhaitez un débit élevé, moyennant un niveau de sécurité inférieur,

choisissez **Group 1**. Si vous souhaitez un niveau de sécurité supérieur, moyennant un débit inférieur, choisissez **Group 5**. Par défaut, Group 1 est sélectionné.

- **Phase 1 / Phase 2 Encryption:** sélectionnez une méthode de cryptage pour cette phase: DES, 3DES, AES-128, AES-192 ou AES-256. La méthode de cryptage détermine la longueur de clé utilisée pour crypter et décrypter les paquets ESP. Il est recommandé de choisir AES-256, car cette méthode est plus sûre.
- **Phase 1 / Phase 2 Authentication:** sélectionnez une méthode d'authentification pour cette phase (MD5 ou SHA1). La méthode d'authentification détermine la manière dont les paquets d'en-tête ESP (Encapsulating Security Payload) sont validés. MD5 est un algorithme de hachage unidirectionnel qui produit une assimilation128bits. SHA1 est un algorithme de hachage unidirectionnel qui produit une assimilation160bits. SHA1 est recommandé, car il est plus sûr. Assurez-vous que les deux extrémités du tunnel VPN utilisent la même méthode d'authentification.
- **Phase 1 / Phase 2 SA Life Time:** configurez la durée pendant laquelle le tunnel VPN est actif, dans cette phase. La valeur par défaut de la Phase1 est de 28800secondes. La valeur par défaut de la Phase2 est de 3600secondes.
- **Perfect Forward Secrecy:** si la fonction PFS (Perfect Forward Secrecy, confidentialité de transmission parfaite) est activée, la négociation IKE de phase2 génère de nouvelles clés destinées au cryptage et à l'authentification du trafic IP. Les pirates informatiques lançant des attaques en force, afin d'obtenir les clés de cryptage, ne sont ainsi pas en mesure d'obtenir les futures clés IPSec. Cochez ou décochez cette case pour activer ou désactiver cette fonction. L'activation de cette fonction est recommandée.
- **Preshared Key:** saisissez la clé prépartagée à utiliser pour l'authentification de l'homologue IKE distant. Vous pouvez saisir jusqu'à 30valeurs hexadécimales etcaractères (présents sur les claviers standard). Ce peut être My_@123 ou 4d795f40313233, par exemple. Les deux extrémités du tunnel VPN doivent utiliser la même clé prépartagée. Nous vous recommandons vivement de modifier régulièrement la clé prépartagée, afin d'optimiser la sécurité du VPN.
- **Minimum Preshared Key Complexity:** cochez la case **Enable** si vous activez l'option Preshared Key Strength Meter.

- **Preshared Key Strength Meter:** si vous activez l'option Minimum Preshared Key Complexity, cet indicateur vous informe sur le niveau de sécurité de la clé prépartagée. Lorsque vous saisissez une clé prépartagée, des barres colorées apparaissent. La palette de couleurs s'étend du rouge (faible) au vert (élevé), en passant par le jaune (acceptable).

  CONSEIL: saisissez une clé prépartagée complexe contenant plus de huit caractères comprenant des minuscules, des majuscules, des chiffres et des symboles tels que -*^+=.

- **Paramètres avancés du mode IKE with Preshared Key**

  Lorsque le paramètre Keying Mode est réglé sur IKE with Preshared Key, les paramètres avancés sont disponibles. Pour la plupart des utilisateurs, les paramètres de base suffisent. Les utilisateurs expérimentés peuvent afficher les paramètres avancés, en cliquant sur **Advanced +**. Pour masquer ces paramètres, cliquez sur **Advanced -**.

  Important: si vous modifiez les paramètres avancés sur un routeur, assurez-fous de saisir les mêmes paramètres sur l'autre routeur.

  - **Aggressive Mode:** deux modes de négociation des associations de sécurité IKE sont possibles, Main Mode et Aggressive Mode. Si la sécurité du réseau est prioritaire, nous vous recommandons de choisir Main Mode. Si le débit du réseau est prioritaire, nous vous recommandons de choisir Aggressive Mode. Vous pouvez modifier ce paramètre si le paramètre Remote Security Gateway Type est configuré sur *IP Only* ou sur un des types *IP +*. Cochez cette case pour activer l'option Aggressive Mode ou décochez-la pour désactiver l'option Aggressive Mode et activer Main Mode.

    REMARQUE: si le paramètre Remote Security Gateway Type est réglé sur un des types *Dynamic IP*, l'option Aggressive Mode est obligatoire. La case est cochée automatiquement et il n'est pas possible de la décocher.

  - **Compress (Support IP Payload Compression Protocol (IP Comp))**: IP Comp est un protocole réduisant la taille des datagrammes IP. Cochez cette case pour permettre au routeur de proposer la compression lors de l'initiation de connexions. Si l'entité qui répond refuse cette proposition, le routeur ne procède pas à la compression. Lorsque le routeur est l'entité qui répond, il accepte toujours la compression, même si l'option n'est pas activée. Si vous activez cette option sur ce routeur, activez-la également sur le routeur situé à l'autre extrémité du tunnel.

- **Keep Alive:** cette fonction permet au routeur de tenter de rétablir automatiquement la connexion VPN, lorsque celle-ci est rompue. Cochez ou décochez cette case pour activer ou désactiver cette fonction.
- **AH Hash Algorithm:** le protocole AH (Authentication Header, en-tête d'authentification) décrit le format des paquets et les normes par défaut de la structure des paquets. L'utilisation du protocole AH en tant que protocole de sécurité assure une protection étendue jusqu'à l'en-tête IP, afin de vérifier l'intégrité du paquet complet. Cochez cette case pour utiliser cette fonction. Choisissez ensuite une méthode d'authentification (MD5 ou SHA1). MD5 produit une assimilation de 128bits pour authentifier les données de paquets. SHA1 produit une assimilation de 160bits pour authentifier les données de paquets. Le même algorithme doit être utilisé aux deux extrémités du tunnel.
- **NetBIOS Broadcast:** des messages de diffusion NetBIOS sont utilisés dans le cadre de la résolution de noms, sur le réseau Windows, pour identifier les ressources tels que les ordinateurs, les imprimantes et les serveurs de fichiers. Ces messages sont utilisés par certaines applications logicielles et par certaines fonctionnalités Windows, dont le voisinage réseau, par exemple. Le trafic de diffusion LAN n'est généralement pas transféré via un tunnel VPN. Toutefois, vous pouvez cocher cette case pour permettre la rediffusion des NetBIOS d'une extrémité du tunnel à l'autre.
- **NAT Traversal:** grâce à la traduction d'adresses réseau (NAT), les utilisateurs possédant des adresses LAN privées peuvent accéder aux ressources d'Internet en utilisant une adresse IP acheminée publiquement en tant qu'adresse source. Toutefois, concernant le trafic interne, la passerelle NAT ne dispose d'aucune méthode automatique de traduction de l'adresse IP publique vers une destination spécifique du LAN privé. Ce problème entrave le succès des échanges IPsec. Si votre routeur VPN se trouve derrière une passerelle NAT, cochez cette case pour activer le NAT traversal. Décochez la case pour désactiver cette option. Vous devez utiliser le même paramètre sur les deux extrémités du tunnel.
- **DPD (Dead peer detection):** cochez cette case pour permettre au routeur d'envoyer régulièrement des messages HELLO/ACK (bonjour/accusé de réception), afin de vérifier l'état du tunnel VPN. Cette option peut être utilisée lorsqu'elle est activée à chaque extrémité du tunnel

VPN uniquement. Indiquez l'intervalle souhaité entre les messages HELLO/ACK (fréquence d'envoi des messages).

Tunnel Backup: lorsque la fonction DPD détecte que l'homologue distant est indisponible, cette fonction permet au routeur de rétablir le tunnel VPN à l'aide d'une différente adresse IP de l'homologue distant ou à l'aide d'une interface différente du réseau WAN local. Cochez cette case pour activer cette fonction. Saisissez ensuite les paramètres décrits ci-après. Cette fonction est disponible uniquement si la fonction Dead Peer Detection est activée.

Remote Backup IP Address: indiquez une adresse IP de l'homologue distant différente de celle habituellement utilisée ou saisissez de nouveau l'adresse IP WAN déjà indiquée pour la passerelle distante.

Local Interface: choisissez l'interface WAN à utiliser pour rétablir la connexion.

VPN Tunnel Backup Idle Time: ce paramètre est utilisé lors du démarrage du routeur. Si le tunnel principal n'est pas connecté dans l'intervalle spécifié, le tunnel de secours est utilisé. L'intervalle d'inactivité par défaut de cette option est de 30secondes.

- **Split DNS:** grâce à la fonction Split DNS, le routeur peut envoyer certaines requêtes DNS à un serveur DNS donné et d'autres requêtes DNS à un autre serveur DNS, en fonction des noms de domaine spécifiés. Lorsque le routeur reçoit une requête de résolution d'adresse de la part du client, le routeur examine le nom de domaine. S'il correspond à l'un des noms de domaine des paramètres Split DNS, il transmet la requête au serveur DNS spécifié. Dans la négative, la requête est transmise au serveur DNS spécifié dans les paramètres d'interface WAN. Cochez ou décochez cette case pour activer ou désactiver cette fonction.

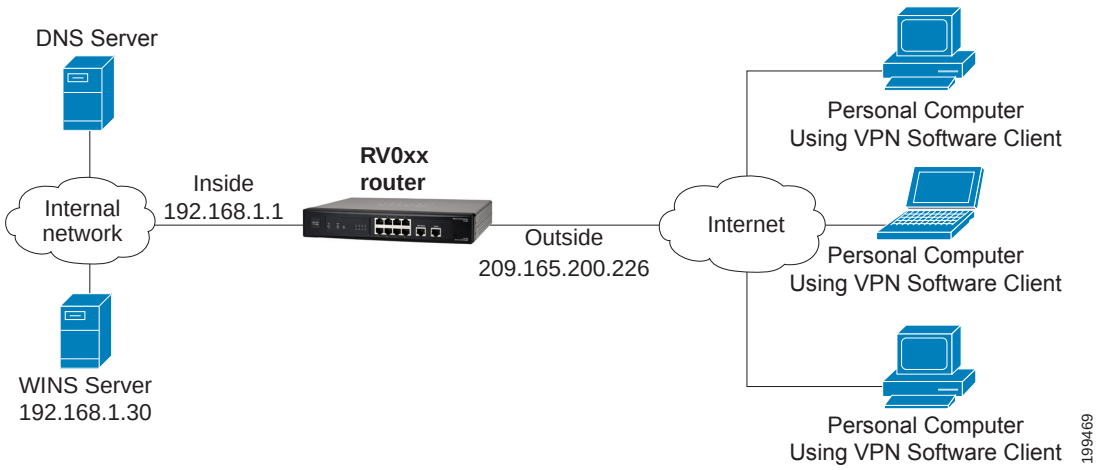
  DNS1: indiquez l'adresselP du serveur DNS à utiliser pour les domaines spécifiés. Vous pouvez également indiquer un serveur DNS secondaire, dans le champ **DNS2** (facultatif).

  Domain Name 1 - Domain Name 4: indiquez les noms de domaine de ces serveurs DNS. Les requêtes destinées à ces domaines sont transmises aux serveurs DNS spécifiés.

Configuration d'un tunnel d'accès à distance pour les clients VPN (client à passerelle)

Utilisez la page *VPN > Client To Gateway* pour créer un nouveau tunnel VPN permettant aux télétravailleurs et aux employés en déplacement d'accéder à votre réseau à l'aide d'un logiciel client VPN tiers tel que TheGreenBow, par exemple.

REMARQUE Pour obtenir plus d'informations sur les clients tiers, voir les notes d'application en visitant le site www.cisco.com/go/smallbizrouters (section *Technical Documentation*).



Pour ouvrir cette page: cliquez sur **VPN> Client to Gateway** dans l'arborescence. Vous pouvez également cliquer sur le bouton **Add Tunnel** de la section *Tunnel Status*, sur la page *VPN > Summary*. Choisissez ensuite **Client to Gateway**.

Add a New Tunnel

Vous pouvez configurer un tunnel VPN pour un seul utilisateur distant ou configurer un VPN de groupe pour plusieurs utilisateurs distants. Vous avez le choix entre deux options:

- **Tunnel:** choisissez cette option si vous souhaitez créer un tunnel pour un seul utilisateur distant. Le numéro du tunnel est généré automatiquement et apparaît dans le champ *Tunnel No*.
- **Group VPN:** choisissez cette option si vous souhaitez créer un tunnel pour un groupe d'utilisateurs. Le VPN de groupe facilite la configuration et élimine la nécessité de configurer les utilisateurs, un à un. Tous les utilisateurs distants peuvent utiliser la même clé pré-partagée pour se connecter au routeur RV0xx, dans la limite du nombre de tunnels pris en charge. Le routeur prend en charge jusqu'à deux VPN de groupe. Le numéro du groupe est généré automatiquement et apparaît dans le champ *Group No*.

Saisissez les informations suivantes:

- **Tunnel Name:** saisissez un nom descriptif du tunnel. Si celui-ci est destiné à un seul utilisateur, vous pouvez saisir le nom ou l'emplacement de cet utilisateur, par exemple. Si le tunnel est destiné à un VPN de groupe, vous pouvez identifier le rôle du groupe au sein de l'entreprise ou son emplacement, par exemple. Cette description sert uniquement de référence et ne doit pas obligatoirement correspondre au nom utilisé à l'autre extrémité du tunnel.
- **Interface:** sélectionnez le port WAN approprié.
- **Enable:** cochez cette case pour activer un VPN de groupe.

Local Group Setup

Saisissez les informations suivantes sur ce routeur.

- **Local Security Gateway Type:** spécifiez la méthode à utiliser pour identifier ce routeur, afin d'établir le tunnel VPN.
  - **IP Only:** choisissez cette option si ce routeur dispose d'une adresse IP WAN statique. L'adresse IP WAN s'affiche automatiquement.
  - **IP + Domain Name (FQDN) Authentication:** choisissez cette option si ce routeur dispose d'une adresse IP statique et d'un nom de domaine inscrit. Saisissez également les paramètres **Domain Name** à utiliser pour l'authentification. Le nom de domaine ne peut être utilisé que pour une seule connexion de tunnel.
  - **IP + E-mail Addr.(USER FQDN) Authentication:** choisissez cette option si ce routeur dispose d'une adresse IP statique et que vous souhaitez utiliser une adresse email pour l'authentification. L'adresse IP WAN actuelle s'affiche automatiquement. Saisissez les adresses email à utiliser pour l'authentification, dans le champ **Email Address**.
  - **Dynamic IP + Domain Name (FQDN) Authentication:** choisissez cette option si ce routeur dispose d'une adresse IP dynamique et d'un nom d'hôte DNS dynamique inscrit (disponible auprès des fournisseurs). Ce peut être DynDNS.com, par exemple. Saisissez le paramètre **Domain Name** à utiliser pour l'authentification. Le nom de domaine ne peut être utilisé que pour une seule connexion de tunnel.
  - **Dynamic IP + E-mail Addr.(USER FQDN) Authentication:** choisissez cette option si ce routeur dispose d'une adresse IP dynamique, mais qu'il n'a pas de nom d'hôte DNS dynamique. Saisissez les adresses email à utiliser pour l'authentification, dans le champ **Email Address**.
- **Local Security Group Type:** spécifiez les ressources LAN pouvant accéder à ce tunnel.
  - **IP Address:** choisissez cette option pour permettre à un seul périphérique LAN d'accéder au tunnel VPN. Saisissez ensuite l'adresse IP de l'ordinateur. Seul ce périphérique peut utiliser ce tunnel VPN.
  - **Subnet:** choisissez cette option (option par défaut) pour autoriser tous les périphériques d'un sous-réseau donné à accéder au tunnel VPN. Saisissez ensuite l'adresse IP de sous-réseau et le masque.
  - **IP Range:** choisissez cette option pour qu'une plage donnée de périphériques puisse accéder au tunnel VPN. Définissez ensuite la plage

d'adresses IP souhaitée. Pour ce faire, saisissez la première adresse de la plage dans le champ **Begin IP** et la dernière adresse de la plage, dans le champ **End IP**.

- **Domain Name**: si vous souhaitez utiliser l'authentification par nom de domaine, saisissez le nom de domaine.
- **Email**: si vous souhaitez utiliser l'authentification par email, saisissez l'adresse email.

Remote Client Setup for Single User (type «Tunnel»)

Spécifiez la méthode à utiliser pour identifier le client, afin d'établir le tunnel VPN. Les options suivantes sont disponibles pour un VPN mono-utilisateur ou de type «Tunnel».

- **IP Only:** choisissez cette option si le client VPN dispose d'une adresse IP WAN statique. Si vous connaissez l'adresse IP du client, choisissez **IP Address**, puis saisissez l'adresse. Si vous ne connaissez pas l'adresse IP du client, choisissez **IP by DNS Resolved**, puis saisissez le nom de domaine réel du client sur Internet. Le routeur obtient l'adresse IP du client VPN distant grâce au paramètre DNS Resolved et l'adresse IP du client VPN distant s'affiche ensuite dans la section VPN Status de la page *Summary*.
- **IP + Domain Name (FQDN) Authentication:** choisissez cette option si ce client dispose d'une adresse IP statique et d'un nom de domaine inscrit. Saisissez également le paramètre **Domain Name** à utiliser pour l'authentification. Le nom de domaine ne peut être utilisé que pour une seule connexion de tunnel.

  Si vous connaissez l'adresse IP du client VPN distant, choisissez **IP Address**, puis saisissez l'adresse. Si vous ne connaissez pas l'adresse IP du client VPN distant, choisissez **IP by DNS Resolved**, puis saisissez le nom de domaine réel du client sur Internet. Le routeur obtient l'adresse IP du client VPN distant grâce au paramètre DNS Resolved et l'adresse IP du client VPN distant s'affiche ensuite dans la section VPN Status de la page *Summary*.
- **IP + Email Address (USER FQDN) Authentication:** choisissez cette option si ce client dispose d'une adresse IP statique et que vous souhaitez utiliser une adresse email pour l'authentification. L'adresse IP WAN actuelle s'affiche automatiquement. Saisissez les adresses email à utiliser pour l'authentification, dans le champ **Email Address**.

Si vous connaissez l'adresse IP du client VPN distant, choisissez **IP Address**, puis saisissez l'adresse. Si vous ne connaissez pas l'adresse IP du client VPN distant, choisissez **IP by DNS Resolved**, puis saisissez le nom de domaine réel du client sur Internet. Le routeur CiscoRV082 obtient l'adresse IP du client VPN distant par la résolution du nom DNS et l'adresse IP du périphérique VPN distant s'affiche ensuite dans la section VPN Status de la page *Summary*.

- **Dynamic IP + Domain Name (FQDN) Authentication:** choisissez cette option si ce client dispose d'une adresse IP dynamique et d'un nom d'hôte DNS dynamique inscrit (disponible auprès des fournisseurs). Ce peut être DynDNS.com, par exemple. Saisissez le paramètre **Domain Name** à utiliser pour l'authentification. Le nom de domaine ne peut être utilisé que pour une seule connexion de tunnel.
- **Dynamic IP + E-mail Addr.(USER FQDN) Authentication:** choisissez cette option si ce client dispose d'une adresse IP dynamique, mais qu'il n'a pas de nom d'hôte DNS dynamique. Saisissez les adresses email à utiliser pour l'authentification, dans le champ **Email Address**.

Remote Client Setup for Single User (type «VPN de groupe»)

Spécifiez la méthode à utiliser pour identifier les clients, afin d'établir le tunnel VPN. Les options suivantes sont disponibles pour un VPN de groupe.

- **Domain Name (FQDN) Authentication:** choisissez cette option pour identifier le client par son nom de domaine inscrit. Saisissez également le paramètre **Domain Name** à utiliser pour l'authentification. Le nom de domaine ne peut être utilisé que pour une seule connexion de tunnel.
- **Email Address (USER FQDN) Authentication:** choisissez cette option pour identifier le client par une adresse email. Saisissez l'adresse dans les champs appropriés.
- **Microsoft XP/2000 VPN Client:** choisissez cette option si le logiciel client est Microsoft XP/2000 VPN Client.

IPSec Setup

Saisissez les paramètres de sécurité du protocole Internet de ce tunnel.

IMPORTANT : afin de permettre tout cryptage, les deux extrémités du tunnel VPN doivent être configurées avec les mêmes méthodes de cryptage, de décryptage et d'authentification.

- **Keying Mode:** choisissez l'une des méthodes de gestion des clés suivantes:
  - **Manual:** choisissez cette option si vous souhaitez générer vous-même la clé et que vous ne souhaitez pas activer la négociation de clé. La gestion manuelle des clés est utilisée dans les petits environnements statiques ou à des fins de dépannage. Saisissez les paramètres souhaités. Pour obtenir plus d'informations, reportez-vous à la section **Champs obligatoires du mode Manual, page 149**.
  - **IKE with Preshared Key:** choisissez cette option si vous souhaitez utiliser le protocole Internet Key Exchange (IKE) pour configurer une association de sécurité, pour votre tunnel. Le protocole IKE utilise une clé prépartagée pour identifier l'homologue IKE distant. Ce paramètre est recommandé et sélectionné par défaut. Saisissez les paramètres souhaités. Pour obtenir plus d'informations, reportez-vous à la section **Champs obligatoires du mode IKE with Preshared Key, page 150** et à la section **Paramètres avancés du mode IKE with Preshared Key, page 152**.
- **Champs obligatoires du mode Manual**

  Saisissez les paramètres du mode Manual.
  - **Incoming / Outgoing SPI:** l'indice des paramètres de sécurité (SPI) se trouve dans l'en-tête du protocole ESP (Encapsulating Security Payload) et permet au récepteur et à l'émetteur de choisir l'association de sécurité à appliquer au traitement des paquets. Vous pouvez saisir des valeurs hexadécimales comprises entre 100 et ffffffff. Chaque tunnel doit avoir un SPI entrant et un SPI sortant uniques. Deux tunnels ne peuvent pas partager le même SPI. La valeur du champ Incoming SPI que vous définissez ici doit être identique à la valeur Outgoing SPI définie à l'autre extrémité du tunnel et vice versa.
  - **Encryption:** sélectionnez une méthode de cryptage (DES ou 3DES). Ce paramètre détermine la longueur de la clé utilisée pour le cryptage ou le décryptage des paquets ESP. DES correspond à un cryptage 56bits et 3DES, à un cryptage 168bits. 3DES est recommandé, car il est plus sûr.

- **Authentication:** sélectionnez une méthode d'authentification (MD5 ou SHA1). La méthode d'authentification détermine la façon dont les paquets ESP sont validés. MD5 est un algorithme de hachage unidirectionnel qui produit une assimilation128bits. SHA1 est un algorithme de hachage unidirectionnel qui produit une assimilation160bits. SHA1 est recommandé, car il est plus sûr. Assurez-vous que les deux extrémités du tunnel VPN utilisent la même méthode d'authentification.
- **Encryption Key:** saisissez la clé à utiliser pour le cryptage et le décryptage du trafic IP. Si vous avez choisi le cryptage DES, saisissez 16valeurs hexadécimales. Si vous avez choisi le cryptage 3DES, saisissez 40valeurs hexadécimales. Si vous ne saisissez pas suffisamment de valeurs hexadécimales, des zéros seront ajoutés à la clé, afin que celle-ci ait la bonne longueur.
- **Authentication Key:** saisissez la clé à utiliser pour authentifier le trafic IP. Si vous avez choisi l'authentification MD5, saisissez 32valeurs hexadécimales. Si vous avez choisi l'authentification SHA1, saisissez 40valeurs hexadécimales. Si vous ne saisissez pas suffisamment de valeurs hexadécimales, des zéros seront ajoutés à la clé, afin que celle-ci ait la bonne longueur.

▪ **Champs obligatoires du mode IKE with Preshared Key**

Saisissez les paramètres des Phases1 et 2. La phase1 consiste à établir les clés prépartagées, afin de créer un canal de communication authentifié et sécurisé. Lors de la Phase2, les homologues IKE utilisent le canal sécurisé pour négocier les associations de sécurité pour le compte d'autres services, tels qu'IPsec.

- **Phase 1 / Phase 2 DH Group:** DH (Diffie-Hellman) est un protocole d'échange de clés. On distingue trois groupes de longueurs de clés primaires: Group1 - 768bits, Group2 - 1024bits et Group5 - 1536bits. Si vous souhaitez un débit élevé, moyennant un niveau de sécurité inférieur, choisissez **Group 1**. Si vous souhaitez un niveau de sécurité supérieur, moyennant un débit inférieur, choisissez **Group 5**. Par défaut, Group 1 est sélectionné.
- **Phase 1 / Phase 2 Encryption:** sélectionnez une méthode de cryptage pour cette phase: DES, 3DES, AES-128, AES-192 ou AES-256. La méthode de cryptage détermine la longueur de clé utilisée pour crypter et décrypter les paquets ESP. Il est recommandé de choisir AES-256, car cette méthode est plus sûre.

- **Phase 1 / Phase 2 Authentication:** sélectionnez une méthode d'authentification pour cette phase (MD5 ou SHA1). La méthode d'authentification détermine la manière dont les paquets d'en-tête ESP (Encapsulating Security Payload) sont validés. MD5 est un algorithme de hachage unidirectionnel qui produit une assimilation128bits. SHA1 est un algorithme de hachage unidirectionnel qui produit une assimilation160bits. SHA1 est recommandé, car il est plus sûr. Assurez-vous que les deux extrémités du tunnel VPN utilisent la même méthode d'authentification.
- **Phase 1 / Phase 2 SA Life Time:** configurez la durée pendant laquelle le tunnel VPN est actif, dans cette phase. La valeur par défaut de la Phase1 est de 28800secondes. La valeur par défaut de la Phase2 est de 3600secondes.
- **Perfect Forward Secrecy:** si la fonction PFS (Perfect Forward Secrecy, confidentialité de transmission parfaite) est activée, la négociation IKE de phase2 génère de nouvelles clés destinées au cryptage et à l'authentification du trafic IP. Les pirates informatiques lançant des attaques en force, afin d'obtenir les clés de cryptage, ne sont ainsi pas en mesure d'obtenir les futures clés IPSec. Cochez ou décochez cette case pour activer ou désactiver cette fonction. L'activation de cette fonction est recommandée.
- **Preshared Key:** saisissez la clé prépartagée à utiliser pour l'authentification de l'homologue IKE distant. Vous pouvez saisir jusqu'à 30valeurs hexadécimales etcaractères (présents sur les claviers standard). Ce peut être My_@123 ou 4d795f40313233, par exemple. Les deux extrémités du tunnel VPN doivent utiliser la même clé prépartagée. Nous vous recommandons vivement de modifier régulièrement la clé prépartagée, afin d'optimiser la sécurité du VPN.
- **Minimum Preshared Key Complexity:** cochez la case **Enable** si vous activez l'option Preshared Key Strength Meter.
- **Preshared Key Strength Meter:** si vous activez l'option Minimum Preshared Key Complexity, cet indicateur vous informe sur le niveau de sécurité de la clé prépartagée. Lorsque vous saisissez une clé prépartagée, des barres colorées apparaissent. La palette de couleurs s'étend du rouge (faible) au vert (élevé), en passant par le jaune (acceptable).

  CONSEIL: saisissez une clé prépartagée complexe contenant plus de huit caractères comprenant des minuscules, des majuscules, des chiffres et des symboles tels que -*^+=.

- **Paramètres avancés du mode IKE with Preshared Key**

  Lorsque le paramètre Keying Mode est réglé sur IKE with Preshared Key, les paramètres avancés sont disponibles. Pour la plupart des utilisateurs, les paramètres de base suffisent. Les utilisateurs expérimentés peuvent afficher les paramètres avancés, en cliquant sur **Advanced +**. Pour masquer ces paramètres, cliquez sur **Advanced -**.

  - **Aggressive Mode** *(disponible pour le tunnel, mais pas pour le VPN de groupe)***:** deux modes de négociation des associations de sécurité IKE sont possibles, Main Mode et Aggressive Mode. Si la sécurité du réseau est prioritaire, nous vous recommandons de choisir Main Mode. Si le débit du réseau est prioritaire, nous vous recommandons de choisir Aggressive Mode. Vous pouvez modifier ce paramètre si le paramètre Remote Security Gateway Type est configuré sur *IP Only* ou sur un des types *IP +*. Cochez cette case pour activer l'option Aggressive Mode ou décochez-la pour désactiver l'option Aggressive Mode et activer Main Mode.

    REMARQUE: si le paramètre Remote Security Gateway Type est réglé sur un des types *Dynamic IP*, l'option Aggressive Mode est obligatoire. La case est cochée automatiquement et il n'est pas possible de la décocher.

  - **Compress (Support IP Payload Compression Protocol (IP Comp))**: IP Comp est un protocole réduisant la taille des datagrammes IP. Cochez cette case pour permettre au routeur de proposer la compression lors de l'initiation de connexions. Si l'entité qui répond refuse cette proposition, le routeur ne procède pas à la compression. Lorsque le périphérique est l'entité qui répond, il accepte toujours la compression, même si l'option n'est pas activée. Si vous activez cette fonctionnalité sur ce routeur, activez-la également sur le client.

  - **Keep Alive :** cette fonction permet au routeur de tenter de rétablir automatiquement la connexion VPN, lorsque celle-ci est rompue. Cochez ou décochez cette case pour activer ou désactiver cette fonction.

  - **AH Hash Algorithm:** le protocole AH (Authentication Header, en-tête d'authentification) décrit le format des paquets et les normes par défaut de la structure des paquets. L'utilisation du protocole AH en tant que protocole de sécurité assure une protection étendue jusqu'à l'en-tête IP, afin de vérifier l'intégrité du paquet complet. Cochez cette case pour utiliser cette fonction. Choisissez ensuite une méthode d'authentification (MD5 ou SHA1). MD5 produit une assimilation de 128bits pour authentifier les données de paquets. SHA1 produit une assimilation de

160bits pour authentifier les données de paquets. Le même algorithme doit être utilisé aux deux extrémités du tunnel.

- **NetBIOS Broadcast:** des messages de diffusion NetBIOS sont utilisés dans le cadre de la résolution de noms, sur le réseau Windows, pour identifier les ressources tels que les ordinateurs, les imprimantes et les serveurs de fichiers. Ces messages sont requis par certaines applications logicielles et par certaines fonctionnalités Windows dont le voisinage réseau, par exemple. Le trafic de diffusion LAN n'est généralement pas transféré via un tunnel VPN. Toutefois, vous pouvez cocher cette case pour permettre la rediffusion des NetBIOS d'une extrémité du tunnel à l'autre.
- **Dead Peer Detection (DPD)** *(disponible pour le tunnel, mais pas pour le VPN de groupe)***:** cochez cette case pour permettre au routeur d'envoyer régulièrement des messages HELLO/ACK (bonjour/accusé de réception), afin de vérifier l'état du tunnel VPN. Cette option peut être utilisée lorsqu'elle est activée à chaque extrémité du tunnel VPN uniquement. Indiquez l'intervalle souhaité entre les messages HELLO/ACK (fréquence d'envoi des messages).
- **NAT Traversal:** grâce à la traduction d'adresses réseau (NAT), les utilisateurs possédant des adresses LAN privées peuvent accéder aux ressources d'Internet en utilisant une adresse IP acheminée publiquement en tant qu'adresse source. Toutefois, concernant le trafic interne, la passerelle NAT ne dispose d'aucune méthode automatique de traduction de l'adresse IP publique vers une destination spécifique du LAN privé. Ce problème entrave le succès des échanges IPsec. Si votre routeur VPN se trouve derrière une passerelle NAT, cochez cette case pour activer le NAT traversal. Décochez la case pour désactiver cette option. Vous devez utiliser le même paramètre sur les deux extrémités du tunnel.

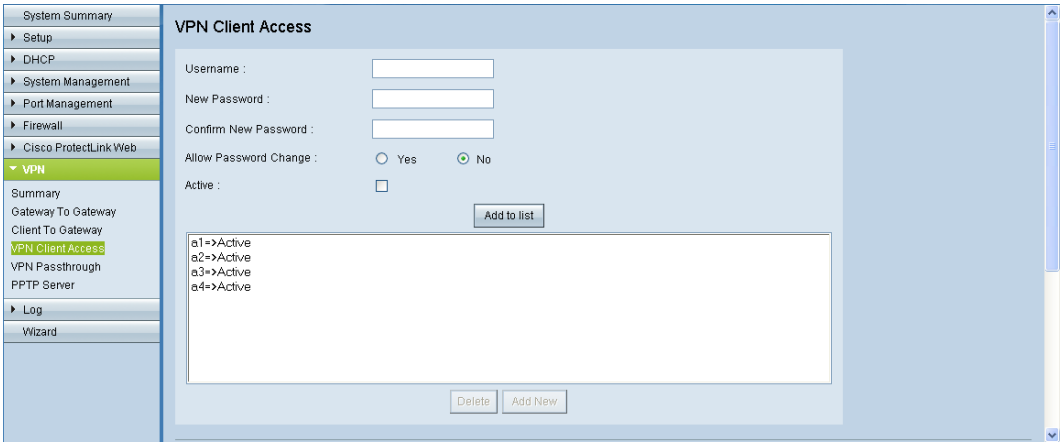
Gestion des utilisateurs et des certificats VPN

Utilisez la page *VPN > Client Access* pour configurer les noms d'utilisateur et les mots de passe pour les utilisateurs Cisco QuickVPN et pour générer les certificats SSL à installer sur leur ordinateur. Vous pouvez ajouter jusqu'à 50utilisateurs. Tout d'abord, exportez un certificat et utilisez le certificat client exporté pour Cisco QuickVPN Client. Saisissez les informations dans la partie supérieure de l'écran; les utilisateurs saisis et leur état apparaissent dans la liste située au bas de l'écran. Le routeur prend en charge jusqu'à 50Cisco QuickVPN Clients.

REMARQUE

- QuickVPN Client version1.4.0.5 et ses versions ultérieures prennent en charge Windows7/XP/Vista. Il est nécessaire d'activer le pare-feu sous Vista et Windows7. Les utilisateurs de QuickVPN doivent disposer de droits d'administrateur sur l'ordinateur.
- Pour que les utilisateurs puissent se connecter, il n'est pas nécessaire d'installer un certificat sur leur ordinateur. L'utilisateur voit s'afficher un avertissement de sécurité, lors de la connexion au tunnel VPN, mais il peut néanmoins continuer sans cette protection supplémentaire.
- Pour plus d'informations sur QuickVPN, reportez-vous à la section **Cisco QuickVPN pour Windows, page 176**.

Pour ouvrir cette page: cliquez sur **VPN> VPN Client Access** dans l'arborescence.



Ajoutez ou mettez à jour les utilisateurs souhaités, selon vos besoins. Pour chaque nouvel utilisateur, exportez un certificat client à installer sur l'ordinateur de l'utilisateur, afin de sécuriser davantage la connexion.

- Users, page 155
- Certificate Management, page 156

REMARQUE Avant de quitter cette page, cliquez sur **Save** pour enregistrer les paramètres ou sur **Cancel** pour les annuler. Les modifications non enregistrées ne sont pas prises en compte.
La première fois que vous enregistrez ces paramètres, un message vous demande si vous souhaitez que le routeur change automatiquement l'adresse IP LAN, afin d'empêcher tout conflit d'adressesIP. Pour changer l'adresse IP LAN, cliquez sur **Yes**. Si un conflit d'adresses IP survient, le client QuickVPN ne se connecte pas au routeur.

Users

- **Pour ajouter un utilisateur VPN à la liste:** saisissez les informations suivantes, puis cliquez sur **Add to list**. Après avoir ajouté des utilisateurs, vous pouvez générer les certificats à installer sur leurs ordinateurs (pour obtenir plus d'informations, reportez-vous à la section **Certificate Management, page 156**).
  - **Username:** saisissez le nom de cet utilisateur.
  - **New Password:** entrez un mot de passe.
  - **Confirm New Password:** saisissez de nouveau le mot de passe, afin de le confirmer.
  - **Allow Password Change:** cochez la case **Yes** pour autoriser l'utilisateur à changer le mot de passe ou cliquez sur **No** pour l'empêcher de changer le mot de passe que vous lui avez attribué.
  - **Active:** cochez cette case pour activer le nouvel utilisateur.
- **Pour ajouter un nouvel utilisateur:** saisissez les informations, puis cliquez sur **Add to list**.
- **Pour modifier un utilisateur dans la liste:** cliquez sur l'entrée à modifier. Les informations apparaissent dans les champs de texte. Apportez les modifications voulues, puis cliquez sur **Update**. Si aucune modification n'est nécessaire, cliquez sur **Add New** pour désélectionner l'entrée et effacer le contenu des champs de texte.
- **Pour supprimer un utilisateur de la liste:** cliquez sur l'entrée à supprimer. Pour sélectionner un bloc d'entrées, cliquez sur la première entrée, maintenez la touche **Maj** enfoncée, puis cliquez sur la dernière entrée du bloc. Pour sélectionner plusieurs entrées individuelles, maintenez la touche **Ctrl** enfoncée tout en cliquant sur les entrées. Cliquez sur **Delete**.

Certificate Management

- **Generate New Certificate:** pour générer un nouveau certificat, afin de remplacer le certificat existant sur le routeur, cliquez sur **Generate**. Lorsque vous cliquez sur ce bouton, une page de confirmation s'affiche. Cliquez sur **OK** pour continuer.
- **Export Certificate for Administrator:** le certificat d'administrateur du routeur contient la clé privée. Vous pouvez exporter une copie du certificat et le sauvegarder. Par exemple, si vous restaurez les paramètres par défaut du routeur, vous devez d'abord exporter le certificat. Après avoir redémarré le routeur, vous pouvez importer ce fichier pour restaurer le certificat. Pour exporter le certificat d'administrateur, cliquez sur **Export for Admin**. Lorsque la fenêtre *File Download* s'affiche, cliquez sur **Save**. Choisissez un emplacement sûr où enregistrer le certificat, saisissez un nom de fichier descriptif et cliquez sur **Save**. Lorsque la fenêtre *Download complete* s'affiche, cliquez sur **Close**.
- **Export Certificate for Client:** vous pouvez installer un certificat client sur l'ordinateur d'un utilisateur, afin de prévenir toute attaque par déni de service. Pour exporter le certificat client, cliquez sur **Export for Client**. Lorsque la fenêtre *File Download* s'affiche, cliquez sur **Save**. Localisez le répertoire d'installation du logiciel client (généralement C:\Program Files\Cisco Small Business\QuickVPN client), saisissez un nom de fichier descriptif et cliquez sur **Save**. Lorsque la fenêtre *Download complete* s'affiche, cliquez sur **Close**.

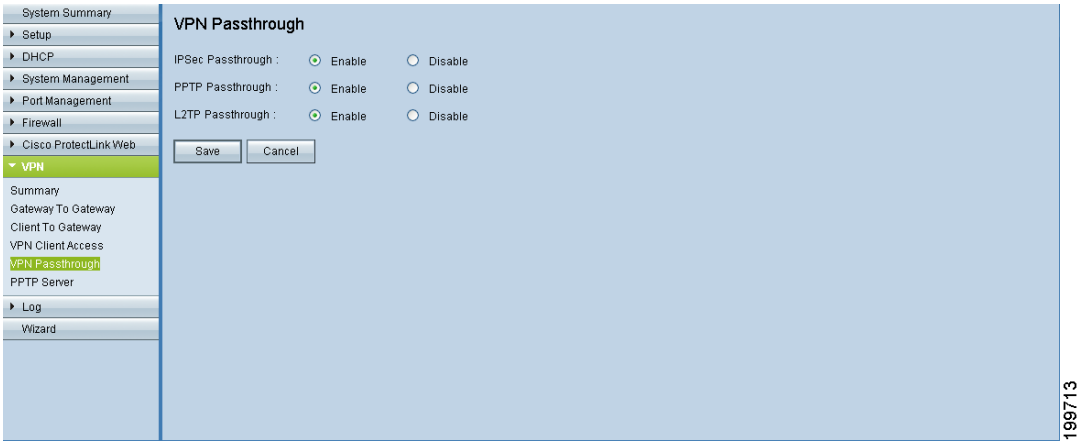
  REMARQUE: pour que les utilisateurs puissent se connecter, il n'est pas nécessaire d'installer un certificat sur leur ordinateur. L'utilisateur voit s'afficher un avertissement de sécurité, lors de la connexion au tunnel VPN, mais il peut néanmoins continuer sans cette protection supplémentaire.
- **Importer le certificat:** pour restaurer un certificat d'administrateur préalablement sauvegardé, cliquez sur **Browse**, localisez le fichier, puis cliquez sur **Open**. Cliquez ensuite sur **Import**. Lorsque le message de confirmation s'affiche, cliquez sur **OK** pour remplacer le certificat existant par le fichier spécifié. Cliquez sur **Cancel** pour fermer le message sans importer le certificat.
- **Existing Certificate:** nom de fichier du certificat actuel enregistré sur le routeur.

Configuration d'un passthrough VPN

Utilisez la page *VPN > VPN Passthrough* pour activer ou désactiver le passthrough de différentes méthodes VPN. Le passthrough VPN est activé par défaut, afin de permettre aux clients VPN situés sur le réseau LAN du routeur de joindre le serveur VPN sur Internet.

Cisco vous recommande d'activer le passthrough VPN afin de permettre aux clients VPN de traverser le routeur pour se connecter sans problème à la terminaison VPN. L'administrateur peut désactiver le passthrough VPN, afin d'empêcher les clients VPN de contacter le point de terminaison VPN sur Internet.

Pour ouvrir cette page: cliquez sur **VPN > VPN Passthrough** dans l'arborescence.



REMARQUE Avant de quitter cette page, cliquez sur **Save** pour enregistrer vos paramètres ou sur **Cancel** pour les annuler. Les modifications non enregistrées ne sont pas prises en compte.

Activez ou désactivez les paramètres suivants, selon vos besoins.

- **IPSec Passthrough:** IPSec (Internet Protocol Security) désigne une série de protocoles utilisés pour sécuriser l'échange des paquets au niveau de la coucheIP. L'option IPSec PassThrough est activée par défaut pour permettre aux tunnels IPSec de traverser le routeur.
- **PPTP Passthrough:** le protocole PPTP (Point-to-Point Tunneling Protocol, protocole de tunnellisation point à point) permet de transmettre le protocole PPP (Point-to-Point Protocol, protocole point à point) via un réseau IP. L'option PPTP PassThrough est activée par défaut.

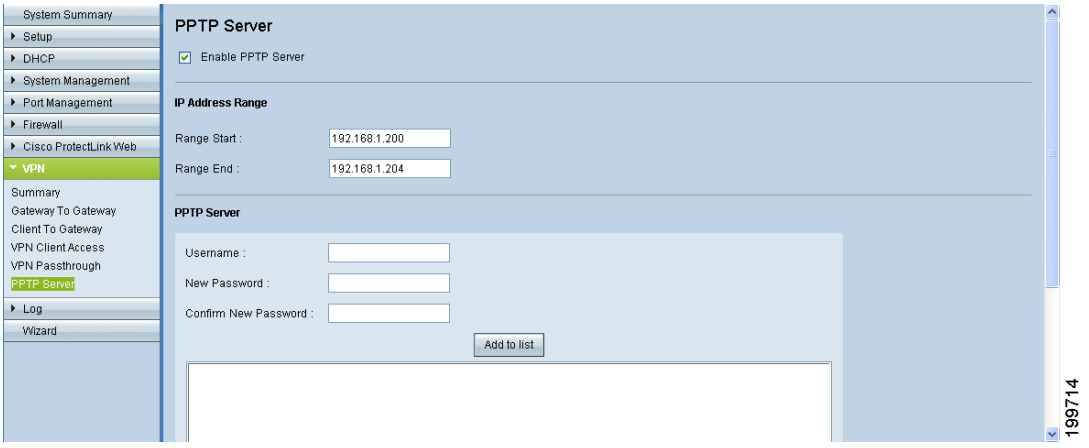
- **L2TP Passthrough:** le protocole L2TP (Layer2 Tunneling Protocol) est la méthode utilisée pour activer des sessions point à point via Internet, au niveau de la couche2. L'option L2TP PassThrough est activée par défaut.

Configuration d'un serveur PPTP

Utilisez la page *VPN > PPTP Server* pour activer jusqu'à cinq tunnels VPN PPTP destinés aux utilisateurs exécutant un logiciel client PPTP sous WindowsXP ou 2000. Les clients PPTP sont inclus par défaut dans Microsoft Windows.

REMARQUE Dans Windows XP/2000, un utilisateur ouvre la fenêtre Connexions réseau et crée une connexion. Dans l'assistant, il choisit l'option qui lui permet de créer une connexion avec son lieu de travail via une connexion de réseau privé virtuel. L'utilisateur devra connaître le nom d'hôte ou l'adresseIP du routeur. Cette valeur doit correspondre à la valeur saisie dans la page *VPN > PPTP Server*. L'assistant indique à l'utilisateur comment créer un raccourci sur le Bureau afin d'exécuter le client. Pour se connecter, l'utilisateur lance le client et ouvre une session en indiquant le nom d'utilisateur et le mot de passe que vous avez définis. Pour plus d'informations, les utilisateurs peuvent consulter la documentation Windows ou les fichiers d'aide.

Pour ouvrir cette page: cliquez sur **VPN > PPTP Server** dans l'arborescence.



REMARQUE Avant de quitter cette page, cliquez sur **Save** pour enregistrer vos paramètres ou sur **Cancel** pour les annuler. Les modifications non enregistrées ne sont pas prises en compte.

Cochez la case **Enable PPTP Server** pour autoriser les tunnels VPN PPTP. Décochez la case pour désactiver cette option. Cette option est désactivée par défaut. Lorsque vous cochez la case, des champs supplémentaires apparaissent.

Plage d'adressesIP

Saisissez la page d'adresses LAN à attribuer aux clients VPN PPTP. Saisissez la première adresse de la plage dans le champ **Range Start** et la dernière adresse, dans le champ **Range End**. La plage par défaut est comprise entre 192.168.1.200 et 92.168.1.204.

REMARQUE La plage d'adresses IP LAN des clients VPN PPTP doit être en dehors de la plage DHCP normale du routeur.

PPTP Server

Vous pouvez ajouter des utilisateurs à la liste des utilisateurs VPN PPTP ou modifier cette liste.

- **Pour ajouter un utilisateur à la liste:** saisissez les informations suivantes, puis cliquez sur **Add to list**.
  - **Username:** saisissez le nom de cet utilisateur.
  - **New Password:** entrez un mot de passe.
  - **Confirm New Password:** saisissez de nouveau le mot de passe, afin de le confirmer.
- **Pour ajouter un nouvel utilisateur:** saisissez les informations, puis cliquez sur **Add to list**.
- **Pour modifier un utilisateur dans la liste:** cliquez sur l'entrée à modifier. Les informations apparaissent dans les champs de texte. Apportez les modifications voulues, puis cliquez sur **Update**. Si aucune modification n'est nécessaire, cliquez sur **Add New** pour désélectionner l'entrée et effacer le contenu des champs de texte.
- **Pour supprimer un utilisateur de la liste:** cliquez sur l'entrée à supprimer. Pour sélectionner un bloc d'entrées, cliquez sur la première entrée, maintenez la touche **Maj** enfoncée, puis cliquez sur la dernière entrée du bloc. Pour sélectionner plusieurs entrées individuelles, maintenez la touche **Ctrl** enfoncée tout en cliquant sur les entrées. Cliquez sur **Delete**.

Connection List

Les informations suivantes apparaissent en lecture seule. Vous pouvez cliquer sur **Refresh** pour mettre à jour les données.

- **Username:** nom du client PPTP VPN.
- **Remote Address:** adresse IP WAN du client VPN PPTP.
- **PPTP IP Address:** adresse IP LAN que le serveur PPTP a attribuée au client, lors de la connexion.

10

Surveillance des statistiques du système

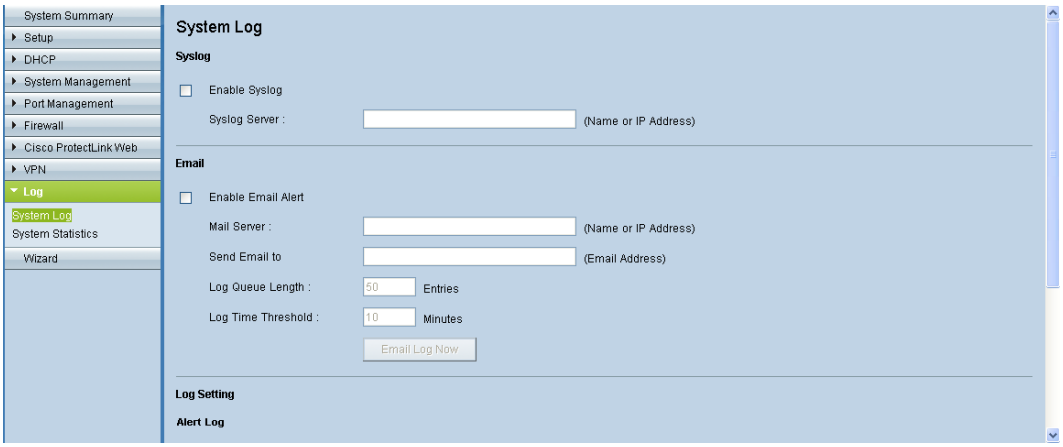
Utilisez le module Log pour configurer le journal système et les alertes et pour afficher les statistiques du système. Reportez-vous aux rubriques suivantes:

- **Configuration du journal système et des alertes, page 161**
- **Affichage du journal système, page 165**

Configuration du journal système et des alertes

Utilisez la page *Log> System Log* pour configurer les journaux et les alertes et pour afficher les tables des journaux.

Pour ouvrir cette page: Cliquez sur **Log> System Log** dans l'arborescence.



REMARQUE Avant de quitter cette page, cliquez sur **Save** pour enregistrer vos paramètres ou sur **Cancel** pour les annuler. Les modifications non enregistrées ne sont pas prises en compte.

Cette page comporte les sections suivantes:

- **Syslog, page 162**

- E-mail, page 162
- Log Setting, page 163
- Buttons, page 164

Syslog

Vous pouvez faire en sorte que le routeur envoie les fichiers journaux détaillés à votre serveur syslog, lorsque des événements sont consignés.

- **Enable Syslog:** Syslog est un protocole standard permettant de collecter des informations sur les activités réseau. Lorsque cette fonctionnalité est activée, le routeur envoie au serveur syslog toutes les activités consignées, y compris les services et les adressesIP source et de destination, dans leur intégralité. Cochez la case pour activer syslog. Décochez la case pour désactiver cette option.
- **Syslog Server:** saisissez le nom ou l'adresseIP du serveur Syslog. Redémarrez le routeur RV0xx pour que les modifications entrent en vigueur.

E-mail

Vous pouvez faire en sorte que le routeur envoie des alertes par e-mail, lorsque des événements sont consignés dans les journaux.

- **Enable E-Mail Alert:** cochez cette case pour que le routeur envoie des alertes par e-mail à l'adresse e-mail spécifiée. Décochez la case pour désactiver cette option.
- **Mail Server:** spécifiez l'adresseIP ou le nom du serveur SMTP de votre fournisseur de services Internet.

  REMARQUE: votre fournisseur de services Internet peut vous demander d'identifier votre routeur en indiquant le nom d'hôte dans la page *Setup> Network*.
- **Send Email to:** saisissez l'adresse e-mail à laquelle vous souhaitez envoyer les alertes.
- **Log Queue Length:** spécifiez le nombre d'entrées de journal à inclure dans l'e-mail. La valeur par défaut est50.
- **Log Time Threshold:** cette valeur représente le temps d'attente maximum avant l'envoi d'un message du journal des e-mails. À l'expiration de ce délai, un e-mail est envoyé, que la mémoire tampon du journal des e-mails soit saturée ou non. Indiquez la durée de la collecte des données, en minutes, avant l'envoi du journal. La valeur par défaut est10.

- **Email Log Now:** cliquez sur ce bouton pour envoyer immédiatement un message à l'adresse e-mail spécifiée, afin de tester vos paramètres.

Log Setting

Choisissez les événements à consigner dans les journaux:

- **Alert Log:** ces événements incluent les types d'attaques classiques, ainsi que les tentatives de connexion non autorisées. Cochez chaque type d'attaque à inclure dans le journal des alertes. Décochez chaque événement à omettre du journal des alertes.
  - **Syn Flooding:** le pirate envoie une succession de paquets SYN, obligeant ainsi le routeur à ouvrir tant de sessions qu'il se retrouve submergé et refuse le service au trafic légitime.
  - **IP Spoofing:** le pirate envoie des paquets avec une adresseIP source falsifiée, afin de déguiser une attaque en trafic légitime.
  - **Win Nuke :** le pirate envoie un message out-of-band à un système Windows, dans l'intention de faire planter l'ordinateur qui le reçoit.
  - **Ping of Death :** le pirate envoie un paquetIP très volumineux, dans l'intention de faire planter l'ordinateur qui le reçoit.
  - **Unauthorized Login Attempt :** une personne essaie d'ouvrir une session dans l'utilitaire de configuration du routeur, mais ne fournit ni le nom d'utilisateur, ni le mot de passe correct.
  - **Output Blocking Event :** un événement s'est produit dans la fonction de réputation Web ou dans la fonction de filtrage des URL de ProtectLink.
- **General Log :** ces événements incluent les actions visant à mettre en place les stratégies configurées, mais aussi les événements tels que les connexions non autorisées et les modifications de la configuration. Cochez chaque type d'événement à inclure dans le journal général. Décochez chaque événement à omettre du journal général.
  - **System Error Messages :** tous les messages d'erreur système.
  - **Deny Policies :** cas où le routeur a refusé l'accès en raison des règles d'accès que vous avez définies.
  - **Allow Policies :** cas où le routeur a autorisé l'accès en raison des règles d'accès que vous avez définies. Notez qu'il est possible d'inclure ou d'exclure du journal, des événements correspondant à des règles d'accès spécifiques, en fonction du paramètre *Log* défini dans la configuration des règles d'accès. Pour obtenir plus d'informations,

reportez-vous à **Configuration des règles d'accès au pare-feu, page 106**.

- **Configuration Changes :** cas où une personne a enregistré des modifications apportées à la configuration.
- **Authorized Login :** cas où une personne a réussi à ouvrir une session dans l'utilitaire de configuration du routeur après avoir spécifié le nom d'utilisateur et le mot de passe corrects.

Buttons

Utilisez ces boutons pour afficher des informations supplémentaires:

- **View System Log :** cliquez sur ce bouton pour afficher le journal système. Les informations du journal s'affichent dans une nouvelle fenêtre. Si le navigateur Web affiche une mise en garde relative à la fenêtre contextuelle, autorisez le contenu bloqué.

  Dans la fenêtre *System Log*, vous pouvez utiliser la liste déroulante pour sélectionner le journal qui vous intéresse. Cliquez sur **Refresh** pour actualiser les données ou sur **Clear** pour faire disparaître toutes les informations affichées. Lorsque vous avez fini de consulter le journal, cliquez sur **Close** pour fermer la fenêtre contextuelle.

  Les entrées du journal contiennent la date et l'heure de l'événement, le type de l'événement et un message. Ce message indique le type de stratégie utilisé, par exemple Access Rule, l'adresse IP du réseau local de la source (SRC) et l'adresse MAC.

- **Outgoing Log Table :** cliquez sur ce bouton pour afficher les informations relatives aux paquets sortants. Les informations sont présentées dans une nouvelle fenêtre.

  Dans la fenêtre *Outgoing Log Table*, vous pouvez cliquer sur **Refresh** pour actualiser les données. Lorsque vous avez fini de consulter le journal, cliquez sur **Close** pour fermer la fenêtre contextuelle.

- **Incoming Log Table :** cliquez sur ce bouton pour afficher les informations relatives aux paquets entrants. Les informations sont présentées dans une nouvelle fenêtre. Si le navigateur Web affiche une mise en garde relative à la fenêtre contextuelle, autorisez le contenu bloqué.

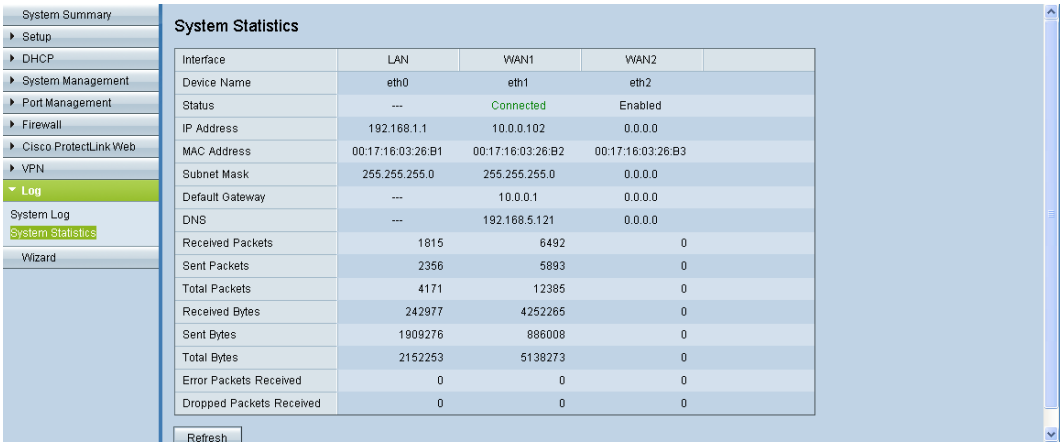
  Dans la fenêtre *Incoming Log Table*, vous pouvez cliquer sur **Refresh** pour actualiser les données. Lorsque vous avez fini de consulter le journal, cliquez sur **Close** pour fermer la fenêtre contextuelle.

- **Clear Log Now :** cliquez sur ce bouton pour vider votre journal sans l'envoyer par e-mail. N'utilisez ce bouton que si vous êtes sûr de ne plus avoir besoin de consulter ces informations.

Affichage du journal système

Utilisez la page *Log> System Log* pour afficher des statistiques au sujet de tous les ports du routeur (LAN et WAN).

Pour ouvrir cette page : cliquez sur **Log> System Statistics** dans l'arborescence.



Des statistiques s'affichent pour chaque interface (LAN, WAN1, WAN2 ou DMZ). Vous pouvez cliquer sur **Refresh** pour mettre à jour les données.

Les statistiques suivantes sont fournies pour chaque port:

- **Device Name :** ID du port, par exemple eth0, eth1, eth2, etc.
- **Status :** état du port. Selon le type d'interface, l'état peut être Connected, Disconnected, Enabled ou Disabled.
- **IP Address :** adresseIP de l'interface.
- **MAC Address :** adresse MAC du périphérique connecté.
- **Subnet Mask :** masque de sous-réseau.
- **Default Gateway :** passerelle par défaut.
- **DNS :** serveur DNS servant à la résolution des noms DNS.

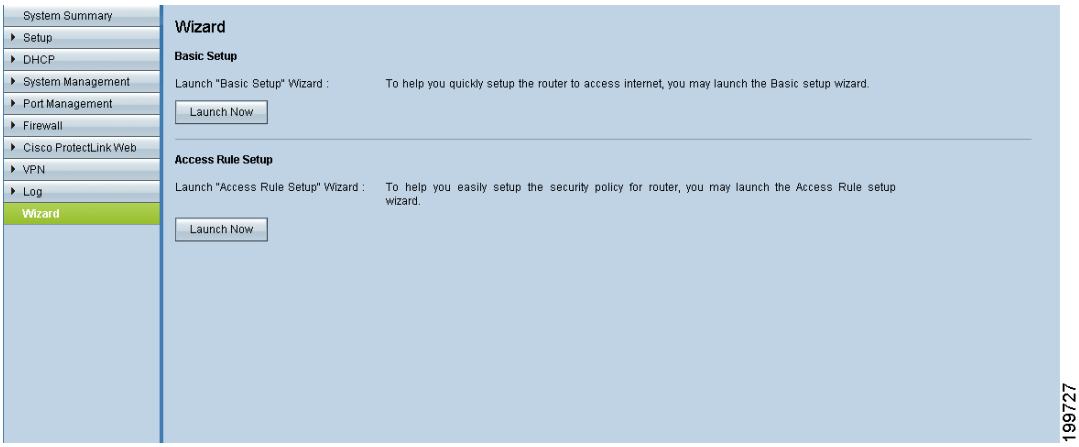
- **Received Packets :** nombre de paquets reçus par le biais de cette interface.
- **Sent Packets :** nombre de paquets envoyés par le biais de cette interface.
- **Total Packets :** nombre total de paquets envoyés et reçus par le biais de cette interface.
- **Received Bytes :** nombre d'octets reçus par le biais de cette interface.
- **Sent Bytes :** nombre d'octets envoyés par le biais de cette interface.
- **Total Bytes :** nombre total d'octets envoyés et reçus par le biais de cette interface.
- **Error Packets Received :** nombre de paquets victimes d'une erreur reçus par le biais de cette interface.
- **Dropped Packets Received :** nombre de paquets reçus et rejetés en raison de problèmes tels qu'une erreur du total de contrôle.

11

Assistant

Utilisez cet onglet pour accéder à deux assistants de configuration: l'assistant de base et l'assistant de configuration des règles d'accès. Exécutez l'assistant de configuration de base pour changer le nombre de portsWAN ou configurer le routeur en fonction de votre ou de vos connexions Internet. Exécutez l'assistant de configuration des règles d'accès pour configurer la stratégie de sécurité du routeur.

Pour ouvrir cette page: Cliquez sur **Wizard** dans l'arborescence. Vous pouvez aussi cliquer sur **Setup Wizard** dans la page *System Summary*.



Cette page comprend les sections suivantes:

- **Basic Setup, page 168**
- **Access Rule Setup, page 168**

Basic Setup

Utilisez l'assistant de configuration de base pour changer le nombre de portsWAN ou pour configurer la connexion Internet.

Cliquez sur **Launch Now** pour exécuter l'assistant de configuration de base. Suivez les instructions à l'écran pour continuer. Reportez-vous aux informations que vous a fournies votre fournisseur de services Internet pour spécifier les paramètres requis par votre connexion.

Access Rule Setup

Utilisez l'assistant de configuration des règles d'accès pour créer les règles d'accès du pare-feu. Cliquez sur **Launch Now** pour exécuter l'assistant de configuration des règles d'accès. Cet assistant fournit des informations sur les règles par défaut du routeur afin de vous aider à démarrer. Suivez les instructions à l'écran pour continuer.

A

Glossaire

Terme	Définition
Beacon Interval	Intervalle de transmission des trames de balise. Les trames de balise indiquent l'existence du réseau sans fil.
DTIM (Delivery Traffic Indication Message)	Un champDTIM 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 multidestination. Après avoir mis en mémoire tampon les messages de diffusion ou de multidestination des clients qui lui sont associés, le routeur Cisco RV220W 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 multidestination.
Dynamic Routing	Le routage dynamique permet au routeur de s'adapter automatiquement aux modifications physiques de la topologie du réseau. Grâce au protocole RIP dynamique, le routeur calcule l'itinéraire le plus efficace pour acheminer les paquets de données du réseau entre la source et la destination. Le protocoleRIP transmet régulièrement les informations de routage aux autres routeurs du réseau. Il détermine le meilleur itinéraire en sélectionnant le plus petit nombre d'étapes entre la source et la destination.

Terme	Définition
Fragmentation Threshold (Seuil de fragmentation)	Longueur de trames, exprimée en octets, permettant de fragmenter en plusieurs trames les paquets qui le nécessitent. Définir une faible valeur permet de réduire les collisions qui se produisent généralement au cours de transmissions de longues trames. Vous devrez utiliser une valeur peu élevée dans les zones pour lesquelles les communications sont mauvaises ou en cas d'interférences de radiofréquences. Un seuil de fragmentation trop bas peut affecter les performances du réseau.
IKE—Internet Key Exchange (échange de clés Internet)	Le protocole IKE échange les clés de manière dynamique entre deux hôtes IPsec.
Mode Préambule	Le standard 802.11b requiert l'ajout d'un préambule à chaque trame pour être transmis sans fil. La transmission d'un long préambule classique dure 192 µs. Un préambule court dure 96 µs. Un long préambule est requis pour assurer la compatibilité avec les systèmes 802.11 fonctionnant à une vitesse de 1 ou 2 Mbps.
RADVD (Démon de notification de routeur)	RADVD est un logiciel Open Source qui utilise le protocole NDP (Neighbor Discovery Protocol) pour écouter les sollicitations du routeur dans le réseau local IPv6. Il répond à d'autres notifications du routeur pour prendre en charge la configuration automatique des adresses sans état. Lorsqu'un nouvel hôte se connecte au réseau, il envoie une demande relative à ses paramètres de configuration et le routeur répond par un paquet de notification de routeur contenant les paramètres de configuration réseau avec les préfixes IPv6. Le nœud extrait le préfixe et l'étend pour obtenir une adresse 128bits complète en ajoutant un EUID à son adresse matérielle.

Terme	Définition
RIPng (RIP next generation)	RIPng est une extension du protocole d'informations de routage, version 2 (RIPv2) pour prendre en charge le protocole IPv6 (reportez-vous à la rubrique RIP dans ce glossaire).
Routage statique	Le routage statique est un chemin prédéterminé qu'emprunte un paquet pour atteindre un hôte ou un réseau donné. **AVERTISSEMENT:** Le routage statique est une fonctionnalité puissante réservée uniquement aux utilisateurs expérimentés. Dans la plupart des cas, il est préférable d'utiliser le routage dynamique car cette fonctionnalité permet au routeur de s'adapter automatiquement aux modifications physiques de la topologie du réseau. Scénarios d'utilisation du routage statique : ▪ Certains fournisseurs d'accès à Internet nécessitent des routes statiques pour construire votre table de routage à la place des protocoles de routage dynamique. ▪ Vous pouvez utiliser des chemins statiques pour atteindre des routeurs homologues qui ne prennent pas en charge les protocoles de routage dynamique. ▪ Si le routeur est connecté à plusieurs réseaux ou que plusieurs routeurs sont installés sur votre réseau, il peut être nécessaire de configurer des itinéraires statiques pour activer le trafic entre eux. ▪ Vous pouvez utiliser le routage statique pour permettre à des utilisateurs de domainesIP différents d'accéder à Internet via le routeur.

Terme	Définition
Routing Information Protocol (RIP)	Ce protocole utilise des vecteurs de distance pour comparer mathématiquement les routages afin d'identifier le meilleur itinéraire pour une adresse de destination donnée. Le protocole RIP envoie des messages de mise à jour de routage à intervalle régulier et lorsque la topologie réseau change. À réception d'un message RIP, un routeur met à jour sa table de routage et transmet les mises à jour vers d'autres routeurs. Le protocole RIP empêche le routage de boucles et possède des fonctions afin d'assurer une certaine stabilité en dépit des évolutions relativement rapides d'une topologie réseau. RIPv2 prend en charge les masques de sous-réseau, permet d'inclure d'autres informations dans les paquets RIP et fournit un mécanisme d'authentification simple non pris en charge par RIP.
Seuil de demande pour émettre (RTS)	La taille du paquet, exprimée en nombre d'octets, nécessite une liaison RTS/Clear to Send (CTS) avant envoi. Un paramètre de faible valeur est préférable dans les zones où de nombreux périphériques clients sont associés à ce périphérique sans fil ou dans les zones où les clients sont si éloignés les uns des autres qu'ils ne détectent que le point d'accès. Bien qu'une valeur de seuil peu élevée consomme plus de bande passante et réduit le débit du paquet, l'envoi de paquets RTS fréquents peuvent contribuer au rétablissement du réseau à l'issue d'interférences ou de collisions.
Taille maximum de l'unité de transfert (MTU)	Paquet le plus grand pouvant être envoyé par le réseau.

Terme	Définition
Traduction d'adresses réseau (NAT)	La traduction d'adresses réseau est une technique qui autorise plusieurs points d'extrémité sur un réseau local à partager une connexion Internet. Dans ce scénario, les ordinateurs du réseau local utilisent une adresse IP « privée » tandis que le port WAN du routeur est configuré avec une seule adresse IP « publique ». Le routeur traduit les adresses privées internes en une adresse publique en masquant les adresses IP internes aux ordinateurs reliés à Internet.
VLAN (LAN virtuels)	Un VLAN est un groupe de points d'extrémité dans un réseau qui sont associés selon leur fonction ou d'autres caractéristiques communes. À la différence des LAN qui sont généralement liés à leur situation géographique, les VLAN peuvent regrouper des points d'extrémité indépendamment de l'emplacement physique du matériel ou des utilisateurs.

B

Résolution des problèmes

La mise à niveau du micrologiciel a échoué.

La mise à niveau du micrologiciel prend environ dix minutes. Une erreur risque de se produire si vous mettez le routeur hors tension, si vous appuyez sur le bouton Reset, si vous fermez la page *System Management> Firmware Upgrade* ou si vous déconnectez l'ordinateur du routeur, pendant la mise à niveau du micrologiciel.

En cas d'échec de la mise à niveau du micrologiciel, répétez la procédure de mise à niveau du micrologiciel, en vous rendant sur la page *System Management> Firmware Upgrade* de l'utilitaire de configuration. Pour obtenir plus d'informations, reportez-vous à **Mise à jour du microprogramme, page 93**.

Si le voyant d'état Diag continue de clignoter, l'image du micrologiciel est endommagée. Utilisez l'utilitaire TFTP pour mettre à niveau le micrologiciel. Vous pouvez télécharger l'utilitaire TFTP à partir du site www.cisco.com.

Votre ordinateur ne parvient pas à se connecter à Internet.

Suivez ces instructions jusqu'à ce que l'ordinateur se connecte à Internet:

- Assurez-vous que le routeur est sous tension. Le voyant d'état System doit être vert et ne doit pas clignoter.
- Si le voyant d'état System clignote, mettez hors tension tous les périphériques réseau, y compris le modem, le routeur et les ordinateurs. Mettez ensuite chaque périphérique sous tension, **dans l'ordre suivant:**
  - Modem câble ou DSL
  - Routeur
  - Ordinateur
- Assurez-vous que les câbles sont correctement branchés. L'ordinateur doit être connecté à l'un des ports du routeur numérotés de 1à4 et le modem doit être connecté au port Internet du routeur.

La prise téléphonique de la ligne DSL ne peut pas être branchée sur le port Internet du routeur.

Le routeur ne remplace pas votre modem. Votre modem DSL reste nécessaire à l'utilisation du routeur. Connectez la ligne téléphonique au modemDSL, insérez le CD-ROM d'installation dans votre ordinateur, puis suivez les instructions affichées à l'écran.

Le routeur n'est pas équipé d'un port coaxial pour la connexion par câble.

Le routeur ne remplace pas votre modem. Votre modem câble reste nécessaire à l'utilisation du routeur. Effectuez la connexion par câble sur le modem câble, insérez le CD-ROM d'installation dans votre ordinateur, puis suivez les instructions affichées à l'écran.

C

Cisco QuickVPN pour Windows

Cisco QuickVPN peut être utilisé pour l'accès des clients à un tunnel Client to Gateway que vous avez configuré sur ce routeur. Reportez-vous aux rubriques suivantes:

- **Introduction, page 176**
- **Installation et configuration du client Cisco QuickVPN, page 177**
- **Utilisation du logiciel Cisco QuickVPN, page 177**

REMARQUE Pour obtenir plus d'informations sur le processus de configuration, reportez-vous à **Gestion des utilisateurs et des certificats VPN, page 154**.

Introduction

Les routeurs VPN Cisco de la gamme RV0xx prennent en charge les logiciels client VPN IPSec, notamment le logiciel Cisco QuickVPN. Pour pouvoir bénéficier des fonctionnalités les plus récentes, merci d'installer QuickVPN Client1.4.0.5 ou version ultérieure, qui prend en charge Windows7.

Le routeur prend en charge gratuitement un maximum de 50clients Cisco QuickVPN. Si votre routeur ne prend en charge que dix clients au maximum, mettez à niveau le micrologiciel du routeur.

Vous pouvez créer un tunnel VPN entre un ordinateur équipé d'un logiciel client VPN et un routeur VPN. La figure suivante est un exemple de VPN établi entre un ordinateur et un routeur VPN. Dans sa chambre d'hôtel, une femme d'affaires en déplacement se connecte à son fournisseur d'accès à Internet (FAI). Sur son ordinateur portable, le logiciel clientVPN est configuré avec les paramètresVPN de son bureau. Elle accède au logiciel client VPN et se connecte au routeur VPN du bureau central. Puisque lesVPN utilisent Internet, la distance ne pose aucun problème. Grâce auVPN, cette personne dispose maintenant d'une connexion sécurisée au réseau du bureau central de sa société, comme si elle y était physiquement connectée.

Installation et configuration du client Cisco QuickVPN

Pour chaque client QuickVPN, procédez comme suit:

STEP 1 Pour télécharger QuickVPN, effectuez les actions suivantes:

a. Ouvrez un navigateur Web, puis saisissez l'adresse suivante: www.cisco.com/go/software

b. Dans la zone Software Download Search, saisissez: **QuickVPN**

c. Cliquez sur **Go**.

d. Dans les résultats de la recherche, cliquez sur le lien correspondant à votre routeur.

e. Suivez les instructions affichées à l'écran pour télécharger le client QuickVPN.

STEP 2 Pour installer le certificat client, enregistrez-le dans le répertoire d'installation du programme QuickVPN.
Exemple: C:\Program Files\Cisco Small Business\QuickVPN Client

REMARQUE: QuickVPN peut être utilisé sans qu'un certificat soit installé sur l'ordinateur. Bien qu'un message d'avertissement relatif à la sécurité s'affiche, l'utilisateur peut tirer parti de QuickVPN sans utiliser cette sécurité supplémentaire.

Utilisation du logiciel Cisco QuickVPN

REMARQUE: un certificat SSL peut également être installé sur l'ordinateur, pour plus de sécurité. Si ce certificat n'est pas installé, vous pouvez néanmoins utiliser QuickVPN, mais un message contextuel d'avertissement s'affiche pendant l'opération.

Pour chaque client QuickVPN, procédez comme suit:

STEP 1 Double-cliquez sur l'icône du logiciel Cisco QuickVPN, sur votre bureau ou dans la barre d'état système.

STEP 2 Lorsque la page *QuickVPN Login* s'affiche, saisissez les informations suivantes:

- **Profile Name:** saisissez le nom de votre profil.

- **Username:** saisissez le nom d'utilisateur qui vous a été attribué.
- **Password:** saisissez le mot de passe qui vous a été attribué.
- **Server Address:** saisissez l'adresse IP WAN ou le nom de domaine du routeur distant.
- **Port for QuickVPN:** saisissez le numéro de port que le client QuickVPN utilisera pour communiquer avec le routeur VPN distant. Vous pouvez également conserver la valeur par défaut, **Auto**.
- **Use Remote DNS Server:** lorsque cette fonctionnalité est activée, les utilisateurs de QuickVPN peuvent se servir du serveur DNS distant (fourni par le serveur QuickVPN) pour résoudre les noms d'hôtes des ordinateurs du sous-réseau distant, sur un tunnel QuickVPN.

STEP 3 Pour enregistrer ce profil, cliquez sur **Save**.

Si vous devez créer un tunnel vers plusieurs sites, vous pouvez créer plusieurs profils. Notez cependant qu'un seul tunnel peut être actif à la fois. Pour supprimer ce profil, cliquez sur **Delete**. Pour obtenir des informations, cliquez sur **Help**.

STEP 4 Pour établir la connexion QuickVPN, cliquez sur **Connect**. La progression de la connexion est affichée dans l'**ordre** suivant: *connexion*, *mise à disposition*, *stratégie d'activation* et *vérification du réseau*.

STEP 5 Une fois que la connexion QuickVPN est établie, l'icône de la barre QuickVPN devient verte et la page *QuickVPN Status* s'affiche. La page présente l'adresse IP de l'extrémité distante du tunnel VPN, la date et l'heure de début du tunnel VPN, ainsi que la durée totale d'activité de ce dernier.

STEP 6 Pour mettre fin au tunnel VPN, cliquez sur **Disconnect**.

Si vous avez cliqué sur Change Password et que vous êtes autorisé à modifier votre propre mot de passe, la page *Connect Virtual Private Connection* s'affiche.

- **Old Password:** saisissez le mot de passe actuel.
- **New Password:** saisissez le nouveau mot de passe.
- **Confirm New Password:** saisissez une deuxième fois ce nouveau mot de passe.

STEP 7 Cliquez sur **OK** pour enregistrer votre nouveau mot de passe. Cliquez sur **Cancel** pour annuler vos modifications. Pour obtenir des informations, cliquez sur **Help**.

REMARQUE Vous ne pouvez modifier votre mot de passe que si votre administrateur système vous a accordé les droits correspondants.

D

Configuration d'un tunnel VPN passerelle à passerelle connecté entre deux routeurs de la gamme RV0xx.

Cette annexe décrit la procédure de configuration d'un VPN entre deux routeurs de la gamme RV0xx. Vous pouvez ensuite réitérer les procédures pour ajouter des tunnels à vos autres sites. Un routeur Cisco de la gamme RV0xx prend en charge jusqu'à 100 tunnels VPN.

REMARQUE Même si vous avez un routeur de la gamme RV0xx sur une extrémité du tunnel et un modèle différent à l'autre extrémité, vous pouvez utiliser ces informations pour configurer votre routeur RV0xx. Notez que les paramètres partagés dont vous avez besoin pour configurer votre autre routeur. Les deux périphériques doivent utiliser une clé commune ou un certificat et comporter des stratégies de sécurité configurées.

Reportez-vous aux rubriques suivantes:

Options de topologie

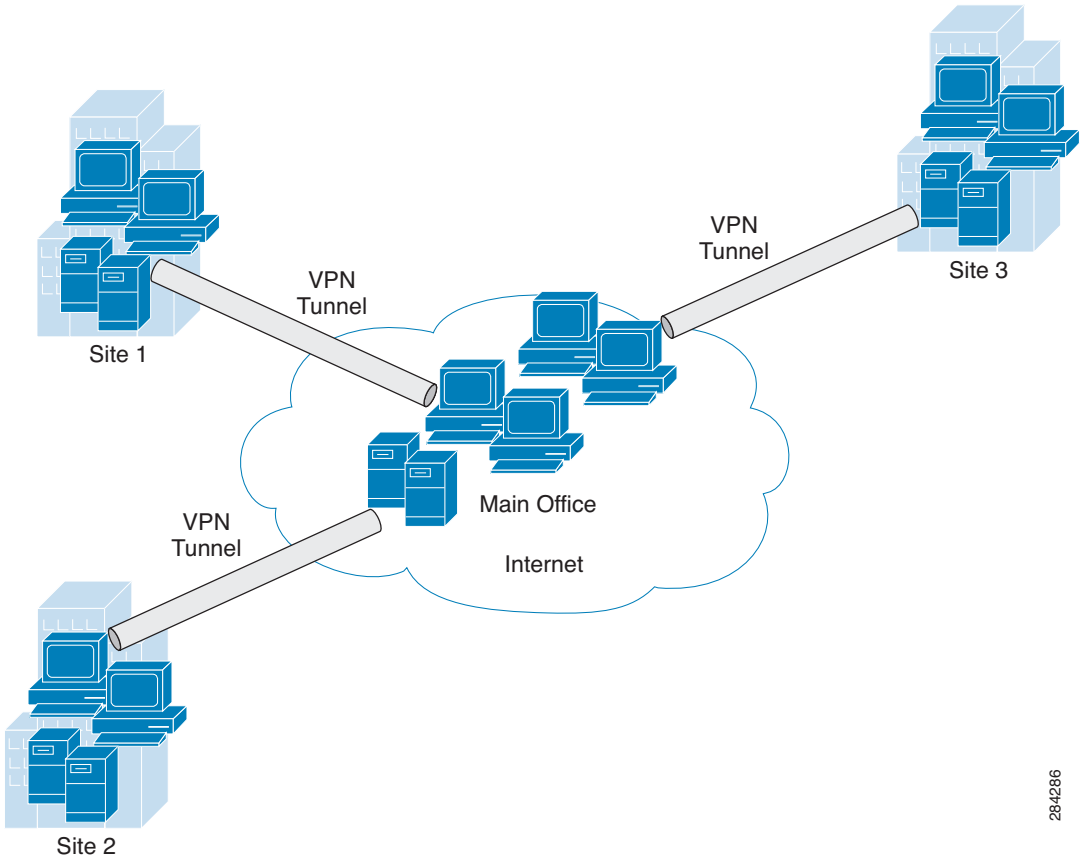
Avant de configurer les paramètres VPN sur vos routeurs, examinez les différentes options de topologie. Une topologie VPN indique les homologues et les réseaux faisant partie du réseau virtuel privé et spécifie la manière dont ils sont reliés entre eux. Selon le nombre de sites et la nature du trafic, vous préférerez une topologie concentrateur/spoke ou une topologie de maillage.

Topologie concentrateur/spoke VPN

Dans une topologie concentrateur/spoke VPN, plusieurs routeurs VPN (spokes) communiquent de manière sécurisée avec un routeur VPN central (concentrateur). Un tunnel sécurisé et indépendant relie chaque spoke au concentrateur.

Dans l'exemple suivant, deux filiales (spokes) disposent de tunnels VPN de site à site avec le bureau central (concentrateur). Le trafic s'effectue généralement entre un site distant et le bureau central. Le trafic entre sites doit d'abord transiter par le concentrateur pour être acheminé vers un spoke.

Concentrateur et spoke



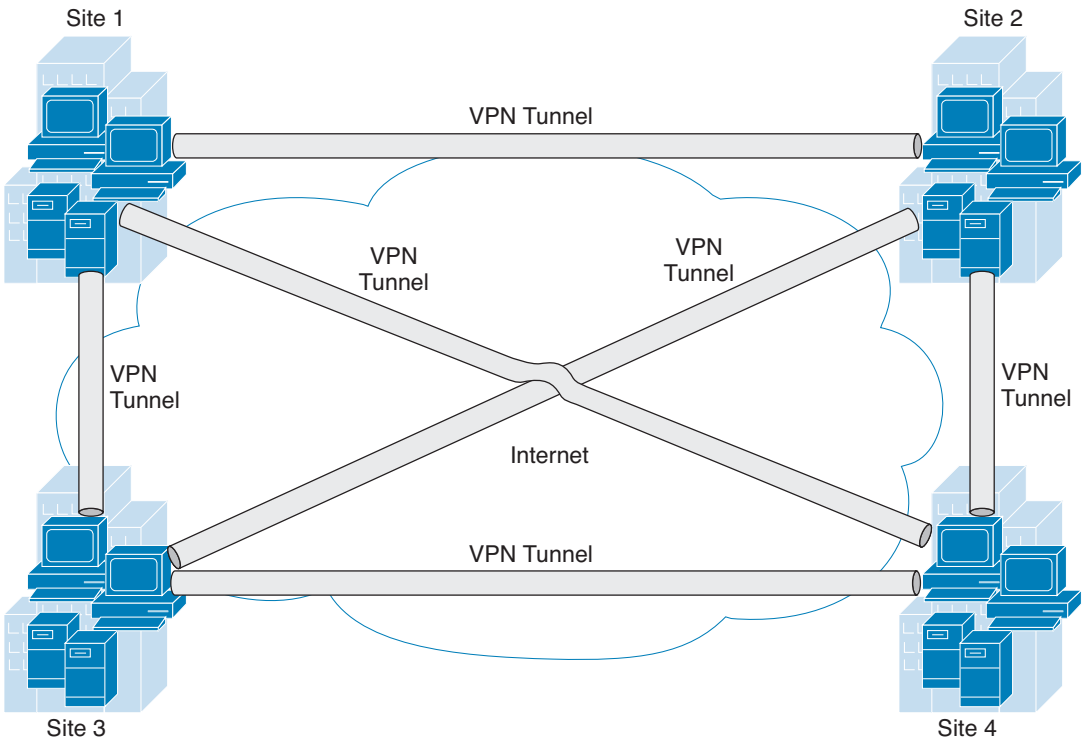
Cette topologie est un outil simple pour autoriser les employés à accéder au réseau central. Il fonctionne correctement si la plupart du trafic va des sites distants vers le réseau central et que le trafic entre les sites est peu important. En effet, un trafic important entre les sites entraînerait des engorgements au niveau du concentrateur.

Topologie de maillage VPN

Dans une topologie de maillage VPN, chaque routeur VPN communique de manière sécurisée avec tous les autres routeurs VPN. Plusieurs tunnels sécurisés relient chaque site à tous les autres sites.

Dans l'exemple suivant, quatre sites sont reliés selon une topologie de maillage VPN. Trois tunnels VPN partent de chaque site et assurent des communications sécurisées vers tous les autres sites. Les données transitent directement entre deux sites.

Conception maillée



Cette topologie nécessite davantage de configuration au niveau de chaque routeur. Toutefois, elle fonctionne bien dans un réseau complexe dans lequel les données sont échangées entre plusieurs sites. Étant donné que tous les périphériques ont des relations directes avec leurs homologues, cette conception empêche les engorgements pouvant survenir au sein d'une topologie concentrateur-spoke. Cette conception garantit également que si un site est inaccessible, les autres sites peuvent continuer d'échanger des données.

REMARQUE Lorsque le nombre de nœuds dans une topologie de maillage VPN augmente, l'évolutivité peut devenir un problème ; le facteur limitatif étant le nombre de tunnels que les périphériques peuvent prendre en charge pour une consommation de la CPU raisonnable.

Autres considérations relatives à la conception

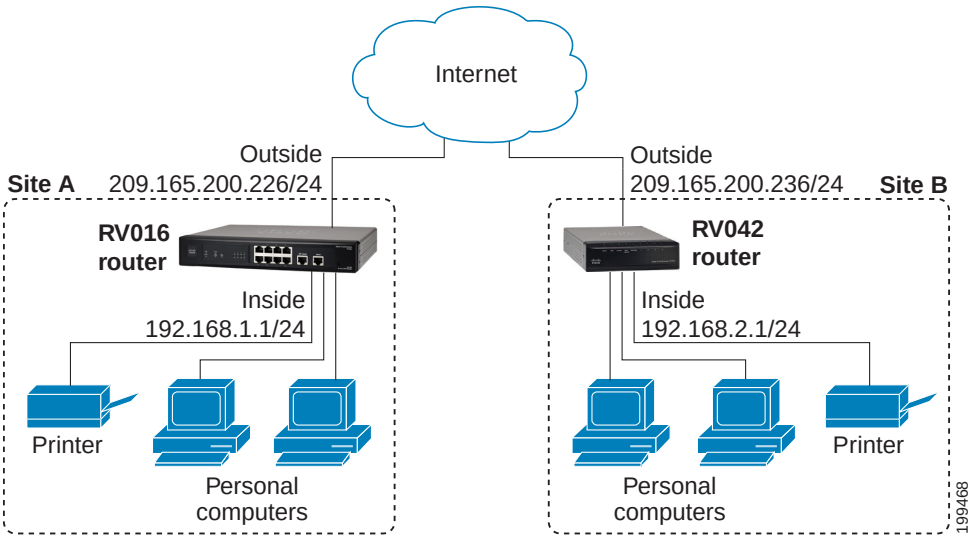
Avant de configurer vos tunnels VPN, considérez les points suivants relativement à votre configuration réseau.

Configuration du réseau WAN

La première considération concerne le type d'adresse IP que vous avez reçues pour votre service Internet au niveau des deux sites. Lors de la construction d'un tunnel ou d'un pont physique, vous devez connaître la destination du tunnel VPN.

- **Si, au moins, un site possède une adresse statique :** Un tunnel VPN peut être facilement établi si au moins un des sites possède une adresse IP statique pour la connexion WAN. Une adresse IP statique est une adresse Internet acheminée publiquement qui ne varie pas. L'établissement d'un tunnel dans ce cas est comparable à la construction d'un pont reliant deux quais (deux sites avec une adresse IP statique) ou d'une passerelle entre un quai et un bateau non amarré (un site avec une adresse IP statique et une avec une adresse IP dynamique).

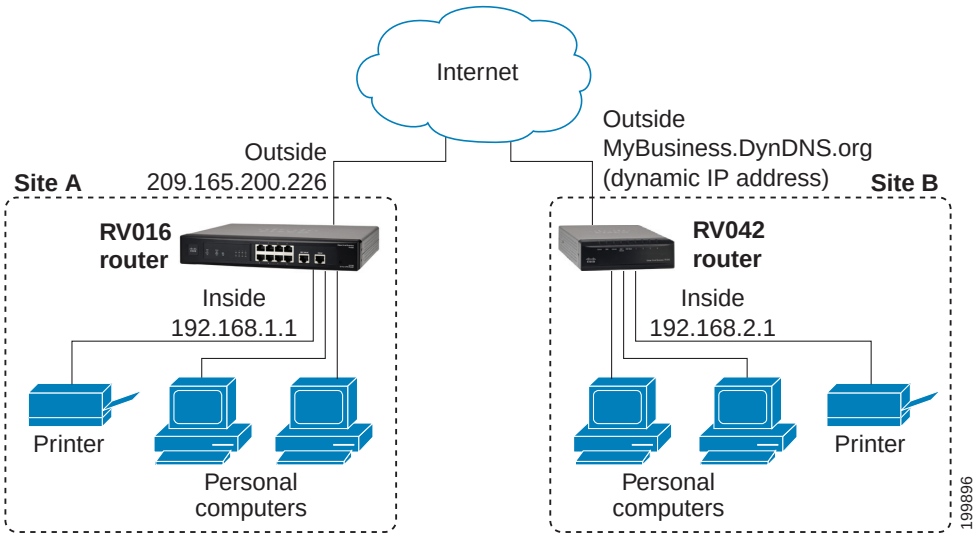
Tunnel passerelle à passerelle avec adresses IP statiques



- **Si les deux sites utilisent des adresses IP dynamiques** Étant donné que les adresses IP dynamiques changent sans préavis, l'établissement d'un tunnel VPN dans ce cas-là revient à essayer de construire un pont entre deux bateaux non amarrés. Toutefois, vous pouvez « amarrer » un bateau, en quelque sorte, en inscrivant au moins un site auprès d'un service Dynamic DNS. Ce service effectue le suivi de votre adresse IP dynamique de sorte que votre routeur reste accessible même si l'adresse change.

  Comme le montre l'illustration ci-dessous, le service Dynamic DNS garantit que le trafic correspondant au nom d'hôte enregistré, MonEntreprise.DynDNS.org, est acheminé vers l'adresse dynamique.

Tunnel passerelle à passerelle avec adresse IP dynamique



Les comptes DNS dynamiques gratuits sont disponibles auprès de nombreux fournisseurs. Voici des exemples:

- http://dyn.com/dyndns
- http://update.ods.org
- http://www.dhs.org
- http://www.3322.org
- http://www.no-ip.com

Configuration du réseau local

Il est nécessaire d'apporter des modifications à votre configuration LAN, sauf si les deux sites ont la même adresse. Les deux extrémités du tunnel ne doivent pas se trouver sur le même sous-réseau. Si, par exemple, l'adresse IP LAN du routeur RV0xx au site A est 192.168.15.1, le site B doit utiliser un autre sous-réseau (192.168.75.1, par exemple).

Configuration d'un tunnel VPN sur un routeur de la gamme CiscoRV0xx

Cette procédure décrit les tâches essentielles de la configuration de votre routeur. La page page 1 donne des exemples de saisie.

STEP 1 Connectez un ordinateur au routeur de gamme Cisco RV0xx (appelé site A dans l'exemple) et lancez l'utilitaire Web de configuration.

STEP 2 Cliquez sur **VPN> Gateway to Gateway** dans l'arborescence.

STEP 3 Saisissez les informations suivantes sur le tunnel:

- **Tunnel Name:** saisissez un nom pour référence. Ce nom s'affiche sur la page *VPN > Summary*.
- **Interface:** sélectionnez l'interface appropriée, **WAN1** ou **WAN2**.

Remarque: la case à cocher **Enable** n'est plus disponible dès que vous avez enregistré la configuration.

STEP 4 Dans la section *Local Group Setup*, saisissez les informations suivantes concernant ce routeur (site A):

- **Local Security Gateway Type :** sélectionnez **IP Only**. L'adresse IP WAN du routeur sera automatiquement détectée et apparaîtra dans le champ *IP Address*.
- **Local Security Group Type :** sélectionnez **IP Only**. Saisissez l'adresse IP LAN dans le champ **IP Address** et le masque de sous-réseau.

STEP 5 Dans la section *Remote Group Setup*, saisissez les informations suivantes concernant à l'autre extrémité du tunnel (site B):

- **Remote Security Gateway Type:**selon le type de l'adresse IP de la connexion Internet, choisissez l'une des options suivantes:
  - *Si la passerelle distante (site B) utilise une adresse IP WAN statique :* sélectionnez **IP Only**. Saisissez l'adresse IP WAN du routeur du siteB dans le champ **IP Address**.
  - *Si la passerelle distante (site B) utilise une adresse IP dynamique ainsi qu'un nom d'hôte DN dynamique :* sélectionnez **Dynamic IP + Domain Name (FQDN) Authentication**. Saisissez le nom de domaine enregistré du routeur du siteB dans le champ **Domain Name** tel que MonEntreprise.DynDNS.org.
- **Remote Security Group Type :** sélectionnez **Subnet**. Saisissez l'adresse IP LAN et le masque de sous-réseau du routeur du siteB dans les champs respectifs **IP Address** et **Subnet Mask**.

STEP 6 Dans la section *IPSec Setup*, conservez les paramètres par défaut (option recommandée) ou saisissez, au besoin, d'autres paramètres : Veillez à configurer le routeur du site B selon les mêmes paramètres.

STEP 7 Dans le champ **Preshared Key**, saisissez une chaîne pour la clé prépartagée, par exemple 13572468. Veillez à configurer l'autre routeur avec la même clé prépartagée.

STEP 8 Pour afficher des paramètres plus détaillés, cliquez sur **Advanced**. Sinon, cliquez sur **Save**.

STEP 9 Sur le site distant (site B), configurez le routeur avec les paramètres correspondants (le site B fait office de passerelle locale et le site A de passerelle distance).

STEP 10 Assurez-vous qu'un ordinateur sur le site A peut effectuer un test ping sur un ordinateur du site B et inversement. Pour obtenir plus d'informations, consultez la rubrique d'aide de Windows. Si le test ping aboutit, le tunnel VPN est correctement configuré.

STEP 11 Recommencez cette procédure pour configurer tout autre tunnel VPN.

Exemple: sites avec adressesIP WAN statiques

Paramètres sur le routeur du site A :

Champ	Valeur
Local Group Setup	
Local Security Gateway Type	IP Only
IP Address	(Détection automatique) 203.165.200.226
Local Security Group Type	Subnet
IP Address	192.168.1.0
Subnet Mask	255.255.255.0
Remote Group Setup	
Remote Security Gateway Type	IP Only
IP Address	209.165.200.238
Remote Security Group Type	Subnet
IP Address	192.168.2.0
Subnet Mask	255.255.255.0
IPSec Setup	
Keying Mode	IKE with Preshared Key
Phase 1 Encryption	DES
Phase 1 Authentication	MD5
Phase 1 SA Life Time	28800

Champ	Valeur
Perfect Forward Secrecy	Enabled
Phase 2 DH Group	Group 1 - 768 bit
Phase 2 Encryption	DES
Phase 2 Authentication	MD5
Phase 2 SA Life Time	3600
Preshared Key	13572468#123456789
Minimum Preshared Key Complexity	Enabled
Advanced	Paramètres par défaut

Paramètres sur le routeur du site B :

Champ	Valeurs
Local Group Setup	
Local Security Gateway Type	IP Only
IP Address	(Détection automatique) 209,165,200,238
Local Security Group Type	Subnet
IP Address	192.168.2.0
Subnet Mask	255.255.255.0

Champ	Valeurs
Remote Group Setup	
Remote Security Gateway Type	IP Only
IP Address	203.165.200.226
Remote Security Group Type	Subnet
IP Address	192.168.1.0
Subnet Mask	255.255.255.0
IPSec Setup	
Keying Mode	IKE with Preshared Key
Phase 1 Encryption	DES
Phase 1 Authentication	MD5
Phase 1 SA Life Time	28800
Perfect Forward Secrecy	Enabled
Phase 2 DH Group	Group 1 - 768 bit
Phase 2 Encryption	DES
Phase 2 Authentication	MD5
Phase 2 SA Life Time	3600
Preshared Key	13572468#123456789
Minimum Preshared Key Complexity	Enabled

Champ	Valeurs
Advanced	Paramètres par défaut

Exemple: site avec adresse IP WAN dynamique

Paramètres sur le routeur du site A :

Champ	Valeur
Local Group Setup	
Local Security Gateway Type	IP Only
IP Address	(Détection automatique) 203.165.200.226
Local Security Group Type	Subnet
IP Address	192.168.1.0
Subnet Mask	255.255.255.0
Remote Group Setup	
Remote Security Gateway Type	Dynamic IP + Domain Name (FQDN) Authentication
Domain Name	cisco.com
Remote Security Group Type	Subnet
IP Address	192.168.2.0
Subnet Mask	255.255.255.0
IPSec Setup	
Keying Mode	IKE with Preshared Key
Phase 1 Encryption	DES

Champ	Valeur
Phase 1 Authentication	MD5
Phase 1 SA Life Time	28800
Perfect Forward Secrecy	Enabled
Phase 2 DH Group	Group 1 - 768 bit
Phase 2 Encryption	DES
Phase 2 Authentication	MD5
Phase 2 SA Life Time	3600
Preshared Key	13572468#123456789
Minimum Preshared Key Complexity	Enabled
Advanced	Paramètres par défaut

Paramètres sur le routeur du site B :

Champ	Valeurs
Local Group Setup	
Local Security Gateway Type	Dynamic IP + Domain Name (FQDN) Authentication
Domain Name	cisco.com
Local Security Group Type	Subnet

Champ	Valeurs
IP Address	192.168.2.0
Subnet Mask	255.255.255.0
Remote Group Setup	
Remote Security Gateway Type	IP Only
IP Address	203.165.200.226
Remote Security Group Type	Subnet
IP Address	192.168.1.0
Subnet Mask	255.255.255.0
IPSec Setup	
Keying Mode	IKE with Preshared Key
Phase 1 Encryption	DES
Phase 1 Authentication	MD5
Phase 1 SA Life Time	28800
Perfect Forward Secrecy	Enabled
Phase 2 DH Group	Group 1 - 768 bit
Phase 2 Encryption	DES
Phase 2 Authentication	MD5
Phase 2 SA Life Time	3600
Preshared Key	13572468#123456789

Champ	Valeurs
Minimum Preshared Key Complexity	Enabled
Advanced	Paramètres par défaut

OL-26286-01

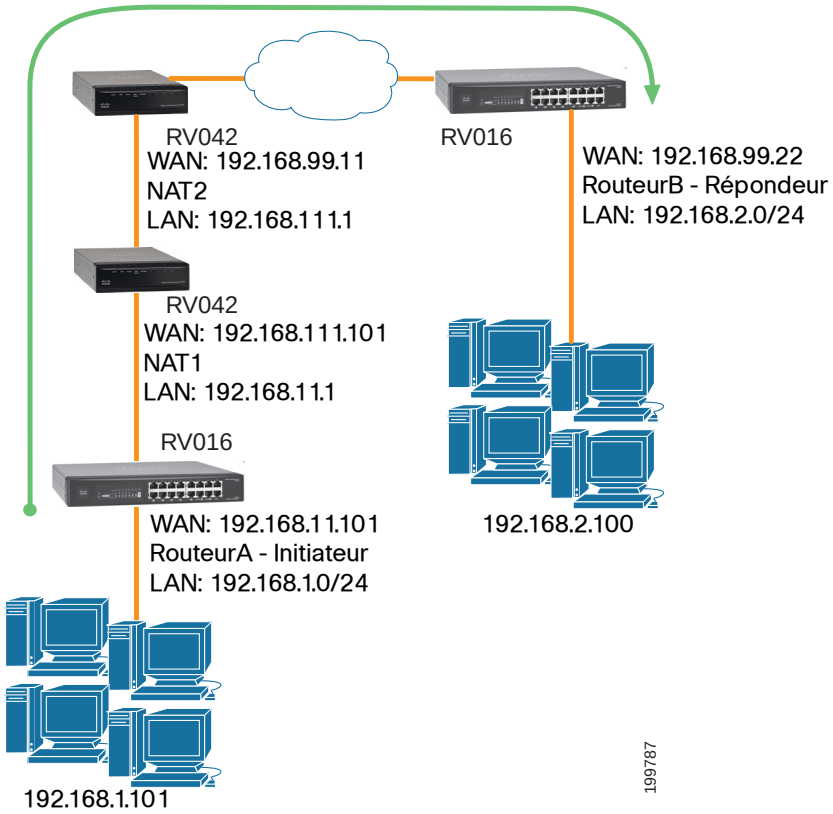
E

Traversée NAT IPsec

Présentation

La technique de traversée NAT (Network Address Translation, traduction d'adresses réseau) a été développée afin que les données protégées par IPSec puissent passer à travers un NAT. Comme IPSec assure l'intégrité de tout le datagramme IP, les données ne sont plus valides si une modification est apportée à l'adressage IP. Pour résoudre ce problème, la traversée NAT ajoute un nouvel en-tête IP et UDP au datagramme entrant pour garantir qu'aucune modification n'est apportée au flux de datagramme entrant.

Dans le scénario suivant, le routeurA initie la négociation IKE et le routeurB est le répondeur.



REMARQUE L'initiateur et le répondeur IPSec doivent prendre en charge le mécanisme de détection du routeur NAT dans le chemin et de passage à un nouveau port, comme défini dans le document RFC3947.

Configuration du routeurA

Suivez ces instructions pour configurer le routeurA.

STEP 1 Lancez le navigateur Web pour un ordinateur en réseau, appelé Ordinateur1.

STEP 2 Accédez à l'utilitaire de configuration du routeurA.

STEP 3 Cliquez sur **VPN> Gateway to Gateway** dans l'arborescence.

STEP 4 Saisissez un nom dans le champ *Tunnel Name*.

STEP 5 Pour le paramètre VPN Tunnel, sélectionnez **Enable**.

STEP 6 Pour Local Security Gateway Type, sélectionnez **IP Only**. L'adresse IP WAN du RouteurA est automatiquement détectée.

Pour Local Security Group Type, sélectionnez **Subnet**. Saisissez les paramètres du réseau local du routeurA dans les champs *IP Address* et *Subnet Mask*.

STEP 7 Pour Remote Security Gateway Type, sélectionnez **IP Only**. Saisissez l'adresse IP WAN du routeurB dans le champ *IP Address*.

STEP 8 Pour Remote Security Group Type, sélectionnez **Subnet**. Saisissez les paramètres du réseau local du routeurB dans les champs *IP Address* et *Subnet Mask*.

STEP 9 Dans la section IPSec Setup, sélectionnez les paramètres appropriés pour le cryptage, l'authentification et d'autres options essentielles de gestion.

STEP 10 Dans le champ *Preshared Key*, saisissez une chaîne pour la clé pré-partagée, par exemple 13572468.

STEP 11 Cliquez sur **Advanced Settings**.

STEP 12 Cochez la case **NAT Traversal** pour activer cette fonctionnalité.

STEP 13 Cliquez sur **Save**.

STEP 14 Passez à la section suivante, **Configuration du routeurB, page 196**.

Configuration du routeurB

Suivez ces instructions pour configurer le routeurB.

STEP 1 Lancez le navigateur Web pour un ordinateur en réseau, appelé Ordinateur2.

STEP 2 Accédez à l'utilitaire de configuration du routeurB.

STEP 3 Cliquez sur **VPN> Gateway to Gateway** dans l'arborescence.

STEP 4 Saisissez un nom dans le champ *Tunnel Name*.

STEP 5 Pour le paramètre VPN Tunnel, sélectionnez **Enable**.

STEP 6 Pour Local Security Gateway Type, sélectionnez **IP Only**. L'adresse IP WAN du RouteurB est automatiquement détectée.

Pour Local Security Group Type, sélectionnez **Subnet**. Saisissez les paramètres du réseau local du routeurB dans les champs *IP Address* et *Subnet Mask*.

STEP 7 Pour Remote Security Gateway Type, sélectionnez **IP Only**. Saisissez l'adresse IP WAN du routeur NAT2 dans le champ *IP Address*.

STEP 8 Pour Remote Security Group Type, sélectionnez **Subnet**. Saisissez les paramètres du réseau local du routeurA dans les champs *IP Address* et *Subnet Mask*.

STEP 9 Dans la section IPSec Setup, sélectionnez les paramètres appropriés pour le cryptage, l'authentification et d'autres options essentielles de gestion.

STEP 10 Dans le champ *Preshared Key*, saisissez une chaîne pour la clé pré-partagée, par exemple 13572468.

STEP 11 Cliquez sur **Advanced Settings**.

STEP 12 Cochez la case **NAT Traversal** pour activer cette fonctionnalité.

STEP 13 Cliquez sur **Save**.

F

Gestion de la bande passante

Ce scénario explique comment garantir la qualité de service (QoS, Quality of Service) du service téléphonique Vonage VoIP (Voix sur IP). Vonage est utilisé dans cet exemple; toutefois, des instructions similaires s'appliquent aux autres services VoIP. Reportez-vous aux rubriques suivantes:

- **Création de nouveaux services, page 198**
- **Création de nouvelles règles de gestion de la bande passante, page 199**

Création de nouveaux services

Créez deux nouveaux services, Vonage VoIP et Vonage2.

STEP 1 Visitez le site Web de Vonage à l'adresse suivante: http://www.vonage.com. Recherchez les ports réservés au service Vonage VoIP.

STEP 2 Accédez à l'utilitaire de configuration du routeur.

STEP 3 Cliquez sur l'onglet **System Management**.

STEP 4 À la page *Bandwidth Management*, cliquez sur **Service Management**.

STEP 5 À la page *Service Management*, saisissez un nom, comme Vonage VoIP, dans le champ *Service Name*.

STEP 6 Dans le menu déroulant *Protocol*, sélectionnez le protocole utilisé par le service VoIP. Par exemple, certains périphériques VoIP utilisent UDP.

STEP 7 Saisissez la plage de ports SIP dans les champs *Port Range*. Par exemple, vous pouvez définir la plage de ports de 5060 à 5070 pour vous assurer que tous les ports actifs sont couverts.

STEP 8 Cliquez sur **Add to List**.

STEP 9 Ajoutez un deuxième service. Saisissez un nom, par exemple Vonage2, dans le champ *Service Name*.

STEP 10 Dans le menu déroulant *Protocol*, sélectionnez **UDP**.

STEP 11 Saisissez la plage de ports RTP dans les champs *Port Range*. Ces paramètres sont requis pour le trafic entrant et sortant. Par exemple, vous pouvez définir la plage de ports de 10000 à 25000 pour vous assurer que tous les ports actifs sont couverts.

STEP 12 Cliquez sur **Add to List**.

STEP 13 Cliquez sur **Save** pour enregistrer vos modifications.

Création de nouvelles règles de gestion de la bande passante

Définissez quatre nouvelles règles: Vonage VoIP (en amont), Vonage VoIP (en aval), Vonage2 (en amont) et Vonage2 (en aval).

STEP 1 Configurez une règle pour la bande passante en amont de Vonage1:

a. À la page *Bandwidth Management*, sélectionnez **Vonage VoIP** dans le menu déroulant *Service*.

b. Saisissez l'adresse IP ou la plage d'adresses IP à contrôler. Pour inclure toutes les adresses IP internes, conservez la valeur par défaut.

c. Dans le menu déroulant *Direction*, sélectionnez **Upstream** pour le trafic sortant.

d. Dans le champ *Min. Rate*, saisissez le débit minimal de la bande passante garantie. Par exemple, vous pouvez définir un débit minimal de 40kbit/s.

e. Dans le champ *Max. Rate*, saisissez le débit maximal de la bande passante garantie. Par exemple, vous pouvez définir un débit maximal de 80kbit/s.

f. Cochez **Enable** pour activer cette règle.

g. Après avoir configuré la règle, cliquez sur **Add to list**.

STEP 2 Configurez la règle s'appliquant à la bande passante en aval de Vonage1:

a. Sélectionnez **Vonage VoIP** dans le menu déroulant *Service*.

b. Saisissez l'adresse IP ou la plage d'adresses IP à contrôler. Pour inclure toutes les adresses IP internes, conservez la valeur par défaut.

c. Dans le menu déroulant *Direction*, sélectionnez **Downstream** pour le trafic entrant.

d. Dans le champ *Min. Rate*, saisissez le débit minimal de la bande passante garantie. Par exemple, vous pouvez définir un débit minimal de 40kbit/s.

e. Dans le champ *Max. Rate*, saisissez le débit maximal de la bande passante garantie. Par exemple, vous pouvez définir un débit maximal de 80kbit/s.

f. Cochez **Enable** pour activer cette règle.

g. Après avoir configuré la règle, cliquez sur **Add to list**.

STEP 3 Configurez une règle en amont pour Vonage2.

a. Sélectionnez **Vonage 2** dans le menu déroulant *Service*.

b. Saisissez l'adresse IP ou la plage d'adresses IP à contrôler. Pour inclure toutes les adresses IP internes, conservez la valeur par défaut, **0**.

c. Dans le menu déroulant *Direction*, sélectionnez **Upstream** pour le trafic sortant.

d. Dans le champ *Min. Rate*, saisissez le débit minimal de la bande passante garantie. Par exemple, vous pouvez définir un débit minimal de 40kbit/s.

e. Dans le champ *Max. Rate*, saisissez le débit maximal de la bande passante garantie. Par exemple, vous pouvez définir un débit maximal de 80kbit/s.

f. Cochez **Enable** pour activer cette règle.

g. Après avoir configuré la règle, cliquez sur **Add to list**.

STEP 4 Configurez une règle en aval pour Vonage2.

a. Sélectionnez **Vonage 2** dans le menu déroulant *Service*.

b. Saisissez l'adresse IP ou la plage d'adresses IP à contrôler. Pour inclure toutes les adresses IP internes, conservez la valeur par défaut, **0**.

c. Dans le menu déroulant *Direction*, sélectionnez **Downstream** pour le trafic entrant.

d. Dans le champ *Min. Rate*, saisissez le débit minimal de la bande passante garantie. Par exemple, vous pouvez définir un débit minimal de 40kbit/s.

e. Dans le champ *Max. Rate*, saisissez le débit maximal de la bande passante garantie. Par exemple, vous pouvez définir un débit maximal de 80kbit/s.

f. Cochez **Enable** pour activer cette règle.

g. Après avoir configuré la règle, cliquez sur **Add to list**.

STEP 5 Cliquez sur **Save**.

G

Caractéristiques

REMARQUE Les caractéristiques peuvent être modifiées sans préavis.

RV042

REMARQUE Ce produit (RV042) est conçu pour être alimenté par un bloc d'alimentation agréé ou de Classe2 et dont la valeur nominale est de 12VCC, 1,0A au minimum.

Caractéristiques	
Modèle	Cisco RV042
Normes	IEEE 802.3, 802.3u
Ports	4 ports 10/100 RJ-45, 1 port Internet
	RJ-45 10/100, 1port DMZ/Internet
	RJ-45 10/100
Bouton	Reset
Type de câblage	Ethernet catégorie 5
Voyants d'état (DEL)	Système, Internet, DMZ/Internet, mode DMZ, diagnostics, 1 à 4
Système d'exploitation	Linux
Performance	
Débit NAT	100Mbits/s
Débit IPSec	59 Mbits/s
Sécurité	
Pare-feu	Pare-feu SPI

Règles d'accès	Jusqu'à 50 entrées
Transfert de port	Jusqu'à 30 entrées
Déclenchement de port	Jusqu'à 30 entrées
Filtrage des URL	Liste d'adresses statiques par domaine ou par mot-clé (incluse), filtrage dynamique par le biais du service Cisco ProtectLink Web (facultatif)
Réseau	
WAN doubles	Peuvent être configurés pour l'équilibrage de la charge ou la sauvegarde Smartlink
Liaison de protocoles	Les protocoles peuvent être associés à un port WAN particulier, pour l'équilibrage de la charge
DHCP	Serveur DHCP, client DHCP
DNS	Proxy DNS, DNS dynamique (DynDNS, 3322)
NAT	Plusieurs-à-un, un-à-un
DMZ	Port DMZ, hôte DMZ
Routage	Statique et RIP v1, v2
QoS	
QoS basée sur les ports	Configurable par port LAN
QoS basée sur les services	Prend en charge la priorité ou le contrôle de débit
Contrôle du débit	Possibilité de configurer la bande passante en amont/aval par service
Priorité	Chaque service peut être mappé sur un des 3niveaux de priorité
VPN	
IPSec 50 tunnels IPSec pour la connectivité entre filiales	
QuickVPN	50 utilisateurs de QuickVPN pour l'accès des clients distants
PPTP	Serveur PPTP intégré prenant en charge 5clients PPTP
Cryptage	DES, 3DES, AES-128, AES-192, AES-256

Authentification	MD5, SHA1
IPSec NAT-T	Pris en charge pour les tunnels passerelle à passerelle et client à passerelle
Passthrough VPN	PPTP, L2TP, IPSec
Gestion	
Web	HTTPS
SNMP	Prend en charge SNMP v1 et v2c
Journaux	journal système, alertes par e-mail
Environnement	
Dimensions	130mm x 38,5mm x 200mm (L x H x P) (5,12"x1,52"x7,87")
Poids	0,576kg (1,27livre)
Alimentation	12V, 1A
Certifications	FCC classe B, CE classe B
Température de fonctionnement	De 0 à 40°C
Température de stockage	De 0 à 70°C
Humidité de fonctionnement	De 10 à 85%, sans condensation
Humidité de stockage	De 5 à 90%, sans condensation

RV042G

REMARQUE Ce produit (RV042G) est conçu pour être alimenté par un bloc d'alimentation agréé ou de Classe2 et dont la valeur nominale est de 12VCC, 1,0A au minimum.

Caractéristiques	
Modèle	Cisco RV042G
Normes	IEEE 802.3, 802.3u
Ports	4 ports 10/100/1000 RJ-45, 1port Internet RJ-45

	10/100/1000, 1port DMZ/Internet
	RJ-45 10/100/1000
Bouton	Reset
Type de câblage	Ethernet catégorie 5
Voyants d'état (DEL)	Système, Internet, DMZ/Internet, mode DMZ, diagnostics, 1 à 4
Système d'exploitation	Linux
Performance	
Débit NAT	100Mbits/s
Débit IPSec	59 Mbits/s
Sécurité	
Pare-feu	Pare-feu SPI
Règles d'accès	Jusqu'à 50 entrées
Transfert de port	Jusqu'à 30 entrées
Déclenchement de port	Jusqu'à 30 entrées
Filtrage des URL	Liste d'adresses statiques par domaine ou par mot-clé (incluse) Remarque : le service Cisco ProtectLink Web n'est pas disponible pour ce modèle.
Réseau	
WAN doubles	Peuvent être configurés pour l'équilibrage de la charge ou la sauvegarde Smartlink
Liaison de protocoles	Les protocoles peuvent être associés à un port WAN particulier, pour l'équilibrage de la charge
DHCP	Serveur DHCP, client DHCP
DNS	Proxy DNS, DNS dynamique (DynDNS, 3322)
NAT	Plusieurs-à-un, un-à-un
DMZ	Port DMZ, hôte DMZ
Routage	Statique et RIP v1, v2

QoS	
QoS basée sur les ports	Configurable par port LAN
QoS basée sur les services	Prend en charge la priorité ou le contrôle de débit
Contrôle du débit	Possibilité de configurer la bande passante en amont/aval par service
Priorité	Chaque service peut être mappé sur un des 3niveaux de priorité
VPN	
IPSec 50 tunnels IPSec pour la connectivité entre filiales	
QuickVPN	50 utilisateurs de QuickVPN pour l'accès des clients distants
PPTP	Serveur PPTP intégré prenant en charge 5clients PPTP
Cryptage	DES, 3DES, AES-128, AES-192, AES-256
Authentification	MD5, SHA1
IPSec NAT-T	Pris en charge pour les tunnels passerelle à passerelle et client à passerelle
Passthrough VPN	PPTP, L2TP, IPSec
Gestion	
Web	HTTPS
SNMP	Prend en charge SNMP v1 et v2c
Journaux	journal système, alertes par e-mail
Environnement	
Dimensions	130 x 38,5 x 200mm (LxHxP) (5,12 x 1,52 x 7,87 ")
Poids	0,576kg (1,27livre)
Alimentation	12V, 1A
Certifications	FCC classe B, CE classe B
Température de fonctionnement	De 0 à 40°C

Température de stockage	De 0 à 70°C
Humidité de fonctionnement	De 10 à 85%, sans condensation
Humidité de stockage	De 5 à 90%, sans condensation

Cisco RV082

Caractéristiques	
Modèle	Routeur VPN 8 ports 10/100 Cisco RV082
Normes	IEEE 802.3, 802.3u
Ports	8ports RJ-45 10/100, 1port Internet RJ-45 10/100, 1port DMZ/Internet RJ-45 10/100
Bouton	Reset
Type de câblage	Ethernet catégorie 5
Voyants d'état (DEL)	Système, Internet, DMZ/Internet, mode DMZ, diagnostics, 1 à 8
Fonctionnalités de sécurité	Pare-feu SPI, cryptage DES, 3DES et AES pour le tunnel VPN IPSec
Système d'exploitation	Linux
Performance	
Débit NAT	200Mbits/s
Débit IPSec	97 Mbits/s
Sécurité	
Pare-feu	Pare-feu SPI
Prévention DoS	Bloque plusieurs attaques de déni de service
Règles d'accès	Jusqu'à 50 entrées
Transfert de port	Jusqu'à 30 entrées
Déclenchement de port	Jusqu'à 30 entrées

Blocage	Java, cookies, ActiveX, proxy HTTP
Filtrage des URL	Liste d'adresses statiques par domaine ou par mot-clé (incluse), filtrage dynamique par le biais du service Cisco ProtectLink Web (facultatif)
Réseau	
WAN doubles	Peuvent être configurés pour l'équilibrage de la charge ou la sauvegarde Smartlink
Type de WAN	DHCP, IP statique, PPPoE, PPTP, DNS dynamique
Liaison de protocoles	Les protocoles peuvent être associés à un port WAN particulier, pour l'équilibrage de la charge
DHCP	Serveur DHCP, client DHCP, relais DHCP
DNS	Proxy DNS, DNS dynamique (DynDNS, 3322)
NAT	Plusieurs-à-un, un-à-un
DMZ	Port DMZ, hôte DMZ
Routage	Statique et RIP v1, v2
QoS	
QoS basée sur les ports	Configurable par port LAN
QoS basée sur les services	Prend en charge la priorité ou le contrôle de débit
Contrôle du débit	Possibilité de configurer la bande passante en amont/aval par service
Priorité	Chaque service peut être mappé sur un des 3niveaux de priorité
VPN	
IPSec	100 tunnels IPSec pour la connectivité entre filiales
QuickVPN	50 utilisateurs de QuickVPN pour l'accès des clients distants
PPTP	Serveur PPTP intégré prenant en charge 5clients PPTP
Cryptage	DES, 3DES, AES-128, AES-192, AES-256
Authentification	MD5, SHA1

IKE	Prend en charge l'échange de clés Internet
IPSec NAT-T	Pris en charge pour les tunnels passerelle à passerelle et client à passerelle
Options avancées	DPD, DNS fractionné, sauvegarde VPN
Passthrough VPN	PPTP, L2TP, IPSec
Gestion	
Web	HTTPS
SNMP	Prend en charge SNMP v1 et v2c
Journaux	Journal système, alertes par e-mail, tunnels VPN, surveillance de l'état
Environnement	
Dimensions	279,4 x 44,45 x 241,3mm (LxHxP) (11,00 x 1,75 x 9,50")
Poids	1,475 kg (3,25livres)
Alimentation	100~240 VCA, 50~60 Hz
Certifications	FCC classe B, CE classe A
Température de fonctionnement	De 0 à 40°C
Température de stockage	De 0 à 70°C
Humidité de fonctionnement	De 10 à 85%, sans condensation
Humidité de stockage	De 5 à 90%, sans condensation

Cisco RV016

Caractéristiques	
Modèle	Routeur VPN 16ports 10/100 Cisco RV016
Normes	IEEE 802.3, 802.3u

Ports	16ports RJ-45 10/100, y compris 2ports Internet, 1 port DMZ, 8ports LAN et 5ports Internet/LAN configurables
Bouton	Reset
Type de câblage	Ethernet catégorie 5
Voyants d'état (DEL)	Diagnostics, système, LAN/Act 1 à 13, Internet/Act 1 à 7, DMZ
Système d'exploitation	Linux
Performance	
Débit NAT	200Mbits/s
Débit IPSec	97 Mbits/s
Sécurité	
Pare-feuPare-feu SPI	
Prévention DoS	Bloque plusieurs attaques de déni de service
Règles d'accès	Jusqu'à 50 entrées
Transfert de port	Jusqu'à 30 entrées
Déclenchement de port	Jusqu'à 30 entrées
Filtrage des URL	Liste d'adresses statiques par domaine ou par mot-clé (incluse), filtrage dynamique par le biais du service Cisco ProtectLink Web (facultatif)
Réseau	
WAN multiples	Prend en charge un maximum de 7ports WAN avec équilibrage de la charge, certains ports WAN pouvant être dédiés à des plages d'adresses IP et à des services spécifiés.
Type de WAN	DHCP, IP statique, PPPoE, PPTP, DNS dynamique
Liaison de protocoles	Les protocoles peuvent être associés à un port WAN particulier
DHCP	Serveur DHCP, client DHCP
DNS	Proxy DNS, DNS dynamique (DynDNS, 3322)
NAT	Plusieurs-à-un, un-à-un

DMZ	Port DMZ, hôte DMZ
Routage	Statique et RIP v1, v2
QoS	
QoS basée sur les ports	Configurable par port LAN
QoS basée sur les services	Prend en charge la priorité ou le contrôle de débit
Contrôle du débit	Possibilité de configurer la bande passante en amont/aval par service
Priorité	Chaque service peut être mappé sur un des 3niveaux de priorité
VPN	
IPSec	100 tunnels IPSec pour la connectivité entre filiales
QuickVPN	50 utilisateurs de QuickVPN pour l'accès des clients distants
PPTP	Serveur PPTP intégré prenant en charge 10clients PPTP
Cryptage	DES, 3DES, AES-128, AES-192, AES-256
Authentification	MD5, SHA1
IKE	Prend en charge l'échange de clés Internet
IPSec NAT-T	Pris en charge pour les tunnels passerelle à passerelle et client à passerelle
Dead Peer Detection	Prise en charge de la détection de l'absence de sites distants (DPD, Dead Peer Detection)
Passthrough VPN	PPTP, L2TP, IPSec
Gestion	
Web	HTTPS
SNMP	Prend en charge SNMP v1 et v2c
Journaux	Journal système, alertes par e-mail, tunnels VPN, surveillance de l'état

Environnement

Dimensions	279,4 x 44,45 x 241,3mm (LxHxP) (11,00 x 1,75 x 9,50")
Poids	1,475 kg (3,25livres)
Alimentation	100~240VCA, 50 à 60Hz
Certifications	FCC classe B, CE classe A
Température de fonctionnement	De 0 à 40°C
Température de stockage	De 0 à 70°C
Humidité de fonctionnement	De 10 à 85%, sans condensation
Humidité de stockage	De 5 à 90%, sans condensation

H

Pour en savoir plus

Cisco fournit un vaste choix de ressources qui vous aident, ainsi que vos clients, à profiter pleinement de tous les avantages de votre routeur Cisco Small Business.

Assistance	
Communauté d'assistance CiscoSmall Business	www.cisco.com/go/smallbizsupport
Ressources et assistance CiscoSmallBusiness	www.cisco.com/go/smallbizhelp
Téléchargements de micrologiciels CiscoSmallBusiness	www.cisco.com/go/software
Documentation sur les produits	
Documentation sur les routeurs Cisco SmallBusiness	www.cisco.com/go/smallbizrouters
CiscoSmallBusiness	
Partenaires et revendeurs Cisco pour les PME (identification partenaire obligatoire)	www.cisco.com/web/partners/sell/smb
Accueil CiscoSmallBusiness	www.cisco.com/smb