Routeur VPN ADSL2+ Wireless-N Cisco RV132W et routeur VPN VDSL2 Wireless-AC RV134W

1

Prise en main

Merci d'avoir choisi le routeur ADSL2+ Wireless-N Cisco RV132W ou les routeurs VDSL2 Wireless-AC Cisco RV134W. Ce guide décrit la procédure à suivre pour installer et gérer votre routeur Cisco RV132W/RV134W. La page **Getting Started** affiche les configurations les plus courantes sur votre appareil. Cliquez sur les liens de la page Web pour accéder à la page de configuration appropriée.

Cette page s'affiche chaque fois que vous démarrez le gestionnaire de périphérique. Pour modifier ce comportement, cochez la case **Don't show on start up**.

Paramètres d'origine

Change Default Administrator Password	Affiche la page **User Account**, dans laquelle vous pouvez modifier le mot de passe administrateur et configurer un compte invité. Reportez-vous à la section **Configuration des comptes d'utilisateurs**.
Launch Setup Wizard	Lance l'**Assistant de configuration du routeur**. Suivez les instructions affichées à l'écran.
Configure WAN Settings	Ouvre la page **Internet Setup**, dans laquelle vous pouvez modifier les paramètres WAN. Reportez-vous à la section **Configuration des connexions WAN**.
Configure LAN Settings	Ouvre la page **LAN Configuration**, dans laquelle vous pouvez modifier les paramètres du réseau LAN. Par exemple, l'adresse IP de gestion. Reportez-vous à la section **Configuration des connexions LAN**.
Configure Wireless Settings	Ouvre la page **Basic Settings** qui permet de gérer les paramètres sans fil. Reportez-vous à la section **Basic Wireless Settings**

Accès rapide

Upgrade Router Firmware	Ouvre la page **Firmware Upgrade** qui permet de mettre à jour le microprogramme de l'appareil. Reportez-vous à la section **Mise à niveau du microprogramme**.
Add VPN Clients (Pour le modèle RV134W uniquement)	Ouvre la page **PPTP Server**, dans laquelle vous pouvez configurer et gérer des tunnels VPN. Reportez-vous à la section **Configuration du protocole PPTP**.
Configure Remote Management Access	Ouvre la page **Basic Settings**, dans laquelle vous pouvez activer les fonctionnalités de base de l'appareil. Reportez-vous à la section **Paramètres de base du pare-feu**.

État de l'appareil

System Summary	Affiche la page **System Summary** qui indique l'état de la configuration IPv4 et IPv6, ainsi que l'état de la connexion sans fil et du pare-feu sur l'appareil. Reportez-vous à la section **System Summary**.
Wireless Status	Affiche la page **Wireless Statistics** qui indique l'état de la radio. Reportez-vous à la section **Wireless Statistics**.
VPN Status (Pour le modèle RV134W uniquement)	Affiche la page **IPsec VPN Server** qui indique le VPN géré par cet appareil. Reportez-vous à la section **PPTP Server**.

Run Setup Wizard

Sur la page **Run Setup Wizard**, vous pouvez suivre les instructions qui vous guident à travers le processus de configuration de l'appareil.

Pour ouvrir cette page, sélectionnez **Run Setup Wizard** dans l'arborescence de navigation.

Suivez les instructions à l'écran pour poursuivre l'opération. Reportez-vous aux informations fournies par votre FAI pour spécifier les paramètres requis par votre connexion Internet.

Connexion au réseau sans fil

Pour connecter un périphérique client (tel qu'un ordinateur) à votre réseau sans fil, vous devez configurer la connexion sans fil sur le périphérique client avec les informations de sécurité sans fil que vous avez configurées pour le routeur à l'aide de l'Assistant de configuration.

Les étapes suivantes sont indiquées à titre d'exemple ; vous pouvez choisir une autre configuration pour votre appareil. Pour obtenir des instructions spécifiques, consultez la documentation de votre périphérique client.

ÉTAPE 1 Ouvrez la fenêtre ou le programme de paramétrage de la connexion sans fil de votre appareil.

Votre ordinateur peut comporter un logiciel spécial pour gérer les connexions sans fil. Vous pouvez également afficher les connexions sans fil dans la fenêtre **Network Connections** ou **Network and Internet** du Panneau de configuration (l'emplacement varie selon le système d'exploitation).

ÉTAPE 2 Saisissez le nom de réseau (SSID) que vous avez choisi pour votre réseau dans l'Assistant de configuration.

ÉTAPE 3 Choisissez le type de cryptage et saisissez la clé de sécurité que vous avez spécifiée dans l'Assistant de configuration.

Si vous n'avez pas activé la sécurité (déconseillé), ne renseignez pas les champs de cryptage sans fil configurés avec le type de sécurité et le mot de passe.

ÉTAPE 4 Vérifiez votre connexion sans fil et enregistrez vos paramètres.

2

État et statistiques

Tableau de bord

Le tableau de bord fournit une vue instantanée des paramètres de configuration sur votre appareil. La page Dashboard affiche des informations sur la version du microprogramme, le numéro de série, l'utilisation du processeur et de la mémoire, les paramètres de journalisation des erreurs, le LAN, le WAN, la connexion sans fil, le VPN IPsec site-à-site et les paramètres de serveur VPN PPTP de votre appareil.

Pour accéder au tableau de bord, sélectionnez **Status and Statistics** > **Dashboard.** Pour modifier les informations affichées, cliquez sur le lien détaillé afin d'accéder à la page de configuration pour cette section. Pour de plus amples informations sur la gestion des paramètres affichés sur la page Dashboard, reportez-vous aux sections suivantes :

- **Configuration des paramètres de journal**
- **VPN site-à-site**
- **Configuration des connexions WAN**
- **Configuration des connexions LAN**

Dans la liste déroulante **Refresh Rate**, choisissez la fréquence à laquelle les dernières statistiques et valeurs de paramètre seront actualisées sur le tableau de bord.

La page Dashboard présente également une vue interactive du panneau arrière de votre appareil lorsque vous cliquez sur **Show Panel View**. Survolez chaque port dont vous souhaitez consulter les informations de connexion avec la souris.

System Summary

Sélectionnez **Status and Statistics** > **System Summary** pour afficher la configuration Internet, le LAN, la connexion sans fil, le pare-feu et le serveur PPTP (pour RV134W).

La page **System Summary** affiche des informations dans les sections suivantes :

WAN Configuration

Affiche les paramètres détaillés de vos réseaux WAN configurés sur la page Networking > WAN > WAN Configuration > Internet Setup. Pour plus d'informations, reportez-vous à la section **Configuration des connexions WAN**.

LAN Configuration

Affiche les paramètres détaillés de vos réseaux LAN configurés sur la page Networking > LAN > LAN Configuration. Pour plus d'informations, reportez-vous à la section **Configuration des connexions LAN**.

Wireless Summary

Affiche le nom public et les paramètres de vos réseaux sans fil configurés sur la page Wireless > Basic Settings. Pour plus d'informations, reportez-vous à la section **Basic Wireless Settings**.

Firewall Setting Status

Affiche les paramètres de DoS (Déni de service), de requête WAN et de gestion à distance configurés sur la page Firewall > Basic Settings > Basic Settings. Pour plus d'informations, reportez-vous à la section **Paramètres de base du pare-feu**.

PPTP Server Status

Affiche les connexions VPN PPTP disponibles, ainsi que les utilisateurs connectés pour chaque type de VPN. Pour plus d'informations sur la configuration des connexions de serveur VPN et des comptes d'utilisateurs, reportez-vous à la section **Configuration du protocole PPTP**.

Active TCP/IP Services

Sélectionnez **Status and Statistics > Active TCP/IP Services** pour afficher les connexions TCP/IP IPv4 et IPv6 qui sont actives sur votre appareil. La section Active Service List pour IPv4 et IPv6 affiche les protocoles et les services actifs sur l'appareil.

Wireless Statistics

Sélectionnez **Status and Statistics** > **Wireless Statistics** pour afficher les données statistiques sans fil de la radio du périphérique. Dans le champ **Refresh Rate**, sélectionnez la fréquence à laquelle vous souhaitez que les dernières statistiques soient affichées.

Pour afficher les octets en kilo-octets (Ko) et les données numériques sous forme de valeurs arrondies, cochez la case **Show Simplified Statistic Data check box** et cliquez sur **Save.** Par défaut, les données d'octets sont affichées en octets et les autres données numériques sont exprimées sous forme développée.

Pour réinitialiser les compteurs de statistiques sans fil, cliquez sur **Clear Count**. Les compteurs sont réinitialisés au redémarrage de l'appareil.

PPTP Server

Sélectionnez **Status and Statistics > PPTP Server** pour afficher la liste de vos connexions VPN PPTP, la durée de la connexion et les actions que vous pouvez effectuer sur cette connexion. Pour plus d'informations sur la configuration des connexions VPN PPTP, reportez-vous à la section **Configuration du protocole PPTP**.

IPSec Connection Status

IPsec VPN Connection Status

ÉTAPE 1 Sélectionnez **Status and Statistics > IPsec Connection Status**.

ÉTAPE 2 Sélectionnez **Refresh Rate** dans la liste déroulante pour afficher les dernières connexions IPSec et la durée de la connexion.

ÉTAPE 3 Sélectionnez l'option **Show Simplified Statistic Data** pour afficher les données statistiques simplifiées.

ÉTAPE 4 Cliquez sur **Save**.

View Logs

La page View Logs n'est visible que si l'utilisateur active le journal dans **Administrator > Logging > Log Setting**. Après avoir activé cette option pour consulter les journaux, sélectionnez **Status and Statistics > View Logs**. Cliquez sur **Refresh Rate** pour afficher les dernières entrées de journal.

Pour filtrer les journaux ou spécifier la gravité des journaux à afficher, dans la table System Log, cochez les cases en regard du type de journal, puis cliquez sur **Go**. Notez que tous les types de journaux au-delà d'un type sélectionné sont automatiquement inclus et qu'il n'est pas possible de les désélectionner. Par exemple, si vous cochez la case Error, vous incluez automatiquement les journaux d'urgence, d'alerte et critiques, en plus des journaux d'erreurs.

Les niveaux de gravité des événements sont répertoriés du niveau le plus élevé au plus faible, comme suit :

- **Emergency** : messages concernant des événements, comme une défaillance système.
- **Alert** : message relatifs à des conditions qui nécessitent une action corrective immédiate.
- **Critical** : messages affichés lorsque le système est dans un état critique.
- **Error** : messages relatifs à des conditions nécessitant une action corrective, sans toutefois être critiques.
- **Warning** : avertissements système.

- **Notification** : messages relatifs à des conditions normales, mais pouvant avoir des conséquences, nécessitant éventuellement une attention particulière.
- **Information** : messages sur les informations du périphérique.
- **Debugging** : informations détaillées sur un événement.

Pour actualiser toutes les entrées de la fenêtre de journaux, cliquez sur **Refresh Logs.**

Pour supprimer toutes les entrées de la fenêtre des journaux, cliquez sur **Clear Logs**.

Pour enregistrer tous les messages de journal du périphérique sur le disque dur local, cliquez sur **Save Logs**.

Pour spécifier le nombre d'entrées à afficher par page, sélectionnez un nombre dans la liste déroulante.

Pour parcourir les pages des journaux, utilisez les boutons de navigation.

Périphériques connectés

La page **Connected Devices** contient des informations sur les périphériques client actifs connectés à votre routeur. Pour afficher les appareils connectés, sélectionnez **Status and Statistics** > **Connected Devices**.

Pour spécifier les types d'interfaces à afficher, sélectionnez une valeur dans la liste déroulante **Filter: Interface Type matches** :

- **All** : tous les périphériques connectés au routeur.
- **Wireless** : tous les périphériques connectés à l'interface sans fil.
- **Wired** : tous les périphériques connectés via les ports Ethernet sur le routeur.

La **Table IPv4 ARP** affiche des informations émanant d'autres routeurs qui ont répondu à la demande ARP (Address Resolution Protocol, protocole de résolution d'adresse) de l'appareil. Si un appareil ne répond pas à la demande, il est supprimé de la liste.

La **table IPv6 NDP** affiche tous les appareils NDP (Neighbor Discover Protocol) IPv6 connectés à la liaison locale de l'appareil.

Port Statistics

La page **Port Statistics** affiche l'activité détaillée des ports.

Pour afficher les statistiques de port, sélectionnez **Status and Statistics > Port Statistics**.

Pour actualiser la page à intervalles réguliers, sélectionnez une fréquence d'actualisation dans la liste déroulante **Refresh Rate**.

Pour afficher les octets en kilo-octets (Ko) et les données numériques sous forme de valeurs arrondies, cochez la case **Show Simplified Statistic Data** et cliquez sur **Save**. Par défaut, les données d'octets sont affichées en octets et les autres données numériques sont exprimées sous forme développée.

Pour réinitialiser les compteurs de statistiques des ports, cliquez sur **Clear Count**.

La page **Port Statistics** affiche les informations suivantes :

Interface	Nom de l'interface réseau.
Packet	Nombre de paquets reçus/envoyés.
Byte	Nombre d'octets reçus/envoyés.
Error	Nombre d'erreurs de paquets reçus/envoyés.
Dropped	Nombre de paquets reçus/envoyés abandonnés.
Multicast	Nombre de paquets en multidiffusion envoyés sur cette radio.
Collisions	Nombre de collisions de signal survenues sur ce port. Une collision survient lorsque le port essaie d'envoyer des données en même temps qu'un port sur un autre routeur ou ordinateur connecté à ce port.

Mobile Network

Statistiques relatives au réseau mobile 3G/4G et à l'appareil de communication (dongle) configuré sur l'appareil.

Pour voir l'état du réseau mobile, sélectionnez **Status and Statistics > Mobile Network**. Les informations suivantes sont indiquées :

- **Connection** : appareil connecté au réseau invité.
- **Internet IP Address** : adresse IP affectée au périphérique USB.
- **Subnet Mask** : masque de sous-réseau du périphérique USB.
- **Default Gateway** : adresse IP de la passerelle par défaut.
- **Connection Up Time** : durée de fonctionnement de la liaison.
- **Current Session Usage** : volume des données reçues (Rx) et transmises (Tx) sur la liaison mobile.
- **Monthly Usage** : données mensuelles téléchargées et utilisation de la bande passante.
- **Manufacturer** : nom du fabricant de la carte.
- **Card Model** : numéro du modèle de la carte.
- **Card Firmware** : version du microprogramme de la carte.
- **SIM Status** : état du module SIM.
- **IMS** : identification unique associée aux utilisateurs de téléphone mobile des réseaux GSM, UMTS ou LTE.
- **Carrier** : porteuse du réseau mobile.
- **Service Type** : type de service auquel vous accédez.
- **Signal Strength** : intensité du signal du réseau mobile sans fil.
- **Card Status** : état de la carte de données.

3

Mise en réseau

Configuration WAN

Configuration des connexions WAN

La configuration des propriétés WAN d'un réseau IPv4 dépend du type de connexion Internet utilisé.

Pour configurer les **Global Settings**, procédez comme suit :

ÉTAPE 1 Sélectionnez **Networking > WAN > WAN Configuration**.

ÉTAPE 2 Dans **Global Settings > Connect Mode**, sélectionnez l'une des options suivantes :

- **Auto** (DSL->Ethernet) : l'appareil vérifie si la liaison DSL est active. Si elle est active, l'appareil l'utilise comme interface WAN. Si elle est inactive, l'appareil vérifie si la liaison Ethernet est active, auquel cas il l'utilise comme interface WAN.
- **DSL** : l'appareil utilise la liaison DSL comme interface WAN.
- **Ethernet :** l'appareil utilise la liaison Ethernet comme interface WAN.

ÉTAPE 3 Cliquez sur **Edit (RV132W) ou sur Add Row (RV134W)** et configurez les paramètres du réseau WAN xDSL ou du réseau WAN Ethernet.

Configuration du réseau WAN xDSL

Lorsque le type de connexion Internet est en mode ponté uniquement :

Dans la section **DSL Settings** du mode de transfert ATM, saisissez les informations suivantes **:**

Mode de transfert	ATM
Multiplexing	Définit la manière dont différents protocoles sont gérés dans un circuit virtuel DSL. Vous pouvez choisir entre une encapsulation LLC (Logical Link Control) et le multiplexage VC (Virtual Channel).
QoS Type	Sélectionnez la qualité de service (QoS) DSL : Unspecified Bit Rate (UBR), Constant Bit Rate (CBR), Variable Bit Rate - real time (VBR-rt), Variable Bit Rate - non-real time (VBR-nrt). CBR offre la meilleure garantie de faible latence : UBR n'en fournit aucune, mais est généralement utilisé pour la plupart des services de données haut débit. **Pcr Rate** : lorsque la qualité de service est définie sur CBR, VBR-rt ou VBR-nrt, saisissez le débit de cellules crête (PCR) en cellules par seconde. **Scr Rate** : lorsque la qualité de service est définie sur VBR-rt ou VBR-nrt, saisissez le taux de cellules retenu (SCR) en cellules par seconde.
Auto Detect	Cochez la case **Enable** pour activer la détection automatique des valeurs VPI et VCI qui identifient votre ligne sur le réseau ATM, ou la case **Disable** pour la désactiver.
Virtual Circuit	Les valeurs **Virtual Path Identifier (VPI)** et **Virtual Channel Identifier (VCI)** sont utilisées pour identifier votre ligne sur le réseau ATM de votre FAI.
SRA (Seamless Rate Adaptation)	Cochez la case **Enable** ou la case **Disable** pour activer ou désactiver le SRA, un protocole qui, en découplant la modulation et la couche de synchronisation, peut modifier les paramètres de vitesse de transmission des données (appliqués par la couche de modulation).
DSL Modulation	Sélectionnez la modulation DSL dans la liste déroulante. La modulation DSL par défaut est **Multimode** (recommandé).

Dans la section **DSL Settings** du mode de transfert PTM (RV134W), saisissez les informations suivantes **:**

Mode de transfert	PTM
SRA (Seamless Rate Adaptation)	Cochez la case **Enable** ou la case **Disable** pour activer ou désactiver le SRA, un protocole qui, en découplant la modulation et la couche de synchronisation, peut modifier les paramètres de vitesse de transmission des données (appliqués par la couche de modulation).
DSL Modulation	Sélectionnez la modulation DSL dans la liste déroulante. La modulation DSL par défaut est **Multimode** (recommandé).

Dans la section **Bridged Settings** des modes de transfert ATM et PTM (RV134W), saisissez les informations suivantes :

Ethernet LAN Ports	Sélectionnez les ports LAN Ethernet (**LAN1, LAN2, LAN3 ou LAN4 -** [RV134W uniquement]).
2.4G Wireless Ports	Sélectionnez **SSID1** (valeur par défaut).
5G Wireless Ports (RV134W uniquement)	Sélectionnez **SSID1** (valeur par défaut).

Dans la section **Other Settings** des modes de transfert ATM et PTM (RV134W), saisissez les informations suivantes **:**

VLAN et VLAN ID	Si cette option est activée, tout le trafic sortant par le biais de cette interface est balisé avec l'ID VLAN configuré**.**
MTU (Maximum Transmission Unit)	MTU est une configuration avancée qui vous permet de déterminer la taille de données maximale autorisée sur votre connexion. Sélectionnez **Auto** (valeur par défaut) ou **Manual** pour configurer les paramètres manuellement.
Size	Saisissez la taille en octets (Plage : 576 - 1 500, valeur par défaut : 1 500).

Lorsque le type de connexion Internet est RFC2684 ponté (mode DHCP ou statique)

Dans la section **DSL Settings** du mode de transfert ATM, saisissez les informations suivantes :

Mode de transfert	ATM
Multiplexing	Définit la manière dont différents protocoles sont gérés dans un circuit virtuel DSL. Vous pouvez choisir entre une encapsulation LLC (Logical Link Control) et le multiplexage VC (Virtual Channel).
QoS Type	Sélectionnez la qualité de service (QoS) DSL : Unspecified Bit Rate (UBR), Constant Bit Rate (CBR), Variable Bit Rate - real time (VBR-rt), Variable Bit Rate - non-real time (VBR-nrt). CBR offre la meilleure garantie de faible latence : UBR n'en fournit aucune, mais est généralement utilisé pour la plupart des services de données haut débit. **Pcr Rate** : lorsque la qualité de service est définie sur CBR, VBR-rt ou VBR-nrt, saisissez le débit de cellules crête (PCR) en cellules par seconde. **Scr Rate** : lorsque la qualité de service est définie sur VBR-rt ou VBR-nrt, saisissez le taux de cellules retenu (SCR) en cellules par seconde.
Auto Detect	Cochez la case **Enable** pour activer la détection automatique des valeurs VPI et VCI qui identifient votre ligne sur le réseau ATM, ou la case **Disable** pour la désactiver.
Virtual Circuit	Les valeurs **Virtual Path Identifier (VPI)** et **Virtual Channel Identifier (VCI)** sont utilisées pour identifier votre ligne sur le réseau ATM de votre FAI.
SRA (Seamless Rate Adaptation)	Cochez la case **Enable** ou la case **Disable** pour activer ou désactiver le SRA, un protocole qui, en découplant la modulation et la couche de synchronisation, peut modifier les paramètres de vitesse de transmission des données (appliqués par la couche de modulation).
DSL Modulation	Sélectionnez la modulation DSL dans la liste déroulante. La modulation DSL par défaut est **Multimode** (recommandé).

Dans la section **DSL Settings** du mode de transfert PTM (RV134W), saisissez les informations suivantes :

Mode de transfert	PTM
SRA (Seamless Rate Adaptation)	Cochez la case **Enable** ou la case **Disable** pour activer ou désactiver le SRA, un protocole qui, en découplant la modulation et la couche de synchronisation, peut modifier les paramètres de vitesse de transmission des données (appliqués par la couche de modulation).
DSL Modulation	Sélectionnez la modulation DSL dans la liste déroulante. La modulation DSL par défaut est **Multimode** (recommandé).

Dans la section **IPoE Settings** des modes de transfert ATM et PTM (RV134W), saisissez les informations suivantes :

Auto Get IP (DHCP)	Cochez la case **Enable** ou la case **Disable** pour activer ou désactiver le paramètre Auto get IP (DHCP), une méthode d'affectation automatique des adresses IP. S'il est désactivé, configurez manuellement l'adresse IP.
DNS Server Source	Sélectionnez **Get Dynamically from ISP** ou **Use These DNS Servers** pour configurer les paramètres manuellement.
Static DNS 1 et 2	Saisissez l'adresse IP du serveur DNS statique principal et/ou secondaire dans les champs (conseil 1.2.3.4).

Dans la section **IPv6 Settings** des modes de transfert ATM et PTM (RV134W), saisissez les informations suivantes :

Pour IPv6

Mode	**IPv6**
Address Mode	Sélectionnez **Dynamic** ou **Static**. Si vous sélectionnez **Dynamic** et que le message RA (Annonce de routeur) reçu par le périphérique contient une balise M « 0 », le périphérique utilise SLAAC (Stateless Address Auto-configuration) pour obtenir les adresses IPv6 ; si la balise M est « 1 », il utilise DHCPv6 pour obtenir l'adresse IPv6. Si vous sélectionnez **Static**, saisissez les informations suivantes : ▪ IPv6 Address ▪ IPv6 Prefix Length ▪ Default IPv6 Gateway ▪ IPv6 DNS1 et DNS2
Prefix Delegation	Pour affecter un préfixe d'adresse réseau (du FAI) au réseau LAN, activez l'option **Prefix Delegation**.

Pour 6rd

Mode	6rd
6rd Tunneling	Sélectionnez **Auto** ou **Manual**. Si vous sélectionnez **Manual**, saisissez les informations suivantes : ▪ IPv6 Prefix ▪ IPv6 Prefix Length ▪ Border Relay ▪ IPv4 Mask Length

Dans la section **Other Settings** des modes de transfert ATM et PTM (RV134W), saisissez les informations suivantes **:**

NAT (Network Address Translation)	Si cette option est activée, tout le trafic sortant par le biais de cette interface est traduit en adresses réseau (NAT). Si elle est désactivée, tout le trafic sortant par le biais de cette interface est acheminé.
VLAN et VLAN ID	Si cette option est activée, tout le trafic sortant par le biais de cette interface est balisé avec l'ID VLAN configuré**.**
802.1p Priority (Pour le mode de transfert ATM uniquement)	Saisissez une plage entre 0 et 7. Tout le trafic sortant de cette interface est balisé avec la priorité 802.1p configurée. S'il entre en conflit avec le paramètre QoS, celui-ci est prioritaire.
MTU (Maximum Transmission Unit)	MTU est une configuration avancée qui vous permet de déterminer la taille de données maximale autorisée sur votre connexion. Sélectionnez **Auto** (valeur par défaut) ou **Manual** pour configurer les paramètres manuellement.
Size	Saisissez la taille en octets (Plage : 576 - 1 500, valeur par défaut : 1 500).
MAC Address Clone	Il peut arriver que vous deviez définir l'adresse MAC du port WAN du périphérique afin qu'il ait la même adresse que votre ordinateur ou une autre adresse MAC. C'est ce que l'on appelle cloner l'adresse MAC. Par exemple, certains FAI enregistrent l'adresse MAC de votre ordinateur lors de l'installation initiale du service. Si vous installez ensuite un routeur derrière le modem câble ou DSL, l'adresse MAC du port WAN du périphérique n'est pas reconnue par le FAI. Pour configurer votre appareil afin qu'il soit reconnu par le FAI, vous pouvez alors cloner l'adresse MAC du port WAN afin qu'elle soit identique à celle de votre ordinateur. Pour configurer un clone d'adresse MAC, sélectionnez **Enable.**

MAC Address	Pour définir l'adresse MAC du port WAN du périphérique, effectuez l'une des opérations suivantes : Pour définir l'adresse MAC du port WAN sur l'adresse MAC de votre PC, cliquez sur **Clone My PC's MAC**. Pour spécifier une autre adresse MAC, saisissez-la dans le champ **MAC Address**.

Lorsque le type de connexion Internet est RFC2684 ponté *(IPoA)*

Dans la section **DSL Settings**, saisissez les informations suivantes :

Mode de transfert	ATM
Multiplexing	Définit la manière dont différents protocoles sont gérés dans un circuit virtuel DSL. Vous pouvez choisir entre une encapsulation LLC (Logical Link Control) et le multiplexage VC (Virtual Channel).
QoS Type	Sélectionnez la qualité de service (QoS) DSL : Unspecified Bit Rate (UBR), Constant Bit Rate (CBR), Variable Bit Rate - real time (VBR-rt), Variable Bit Rate - non-real time (VBR-nrt). CBR offre la meilleure garantie de faible latence : UBR n'en fournit aucune, mais est généralement utilisé pour la plupart des services de données haut débit. **Pcr Rate** : lorsque la qualité de service est définie sur CBR, VBR-rt ou VBR-nrt, saisissez le débit de cellules crête (PCR) en cellules par seconde. **Scr Rate** : lorsque la qualité de service est définie sur VBR-rt ou VBR-nrt, saisissez le taux de cellules retenu (SCR) en cellules par seconde.
Auto Detect	Cochez la case **Enable** pour activer la détection automatique des valeurs VPI et VCI qui identifient votre ligne sur le réseau ATM, ou la case **Disable** pour la désactiver.
Virtual Circuit	Les valeurs **Virtual Path Identifier (VPI)** et **Virtual Channel Identifier (VCI)** sont utilisées pour identifier votre ligne sur le réseau ATM de votre FAI.

SRA (Seamless Rate Adaptation)	Cochez la case **Enable** ou la case **Disable** pour activer ou désactiver le SRA, un protocole qui, en découplant la modulation et la couche de synchronisation, peut modifier les paramètres de vitesse de transmission des données (appliqués par la couche de modulation).
DSL Modulation	Sélectionnez la modulation DSL dans la liste déroulante. La modulation DSL par défaut est **Multimode** (recommandé).

Dans la section **IPoA Settings**, saisissez les informations suivantes **:**

Internet IP Address	Saisissez l'adresse IP (conseil 192.168.100.100).
Subnet Mask	Saisissez le masque de sous-réseau (conseil 255.255.255.0).
Default Gateway	Saisissez la passerelle par défaut (conseil 192.168.100.1).
Static DNS 1 et 2	Saisissez l'adresse IP du serveur DNS statique principal et/ou secondaire dans les champs (conseil 1.2.3.4).

Dans la section **Other Settings**, saisissez les informations suivantes **:**

NAT (Network Address Translation)	Si cette option est activée, tout le trafic sortant par le biais de cette interface est traduit en adresses réseau (NAT). Si elle est désactivée, tout le trafic sortant par le biais de cette interface est acheminé.
MTU (Maximum Transmission Unit)	MTU est une configuration avancée qui vous permet de déterminer la taille de données maximale autorisée sur votre connexion. Sélectionnez **Auto** (valeur par défaut) ou **Manual** pour configurer les paramètres manuellement.
Size	Saisissez la taille en octets (Plage : 576 - 1 500, valeur par défaut : 1 500).

Lorsque le type de connexion Internet est PPPoE :

Dans la section **DSL Settings** du mode de transfert ATM, saisissez les informations suivantes :

Mode de transfert	ATM
Multiplexing	Définit la manière dont différents protocoles sont gérés dans un circuit virtuel DSL. Vous pouvez choisir entre une encapsulation LLC (Logical Link Control) et le multiplexage VC (Virtual Channel).
QoS Type	Sélectionnez la qualité de service (QoS) DSL : Unspecified Bit Rate (UBR), Constant Bit Rate (CBR), Variable Bit Rate - real time (VBR-rt), Variable Bit Rate - non-real time (VBR-nrt). CBR offre la meilleure garantie de faible latence : UBR n'en fournit aucune, mais est généralement utilisé pour la plupart des services de données haut débit. **Pcr Rate** : lorsque la qualité de service est définie sur CBR, VBR-rt ou VBR-nrt, saisissez le débit de cellules crête (PCR) en cellules par seconde. **Scr Rate** : lorsque la qualité de service est définie sur VBR-rt ou VBR-nrt, saisissez le taux de cellules retenu (SCR) en cellules par seconde.
Auto Detect	Cochez la case **Enable** pour activer la détection automatique des valeurs VPI et VCI qui identifient votre ligne sur le réseau ATM, ou la case **Disable** pour la désactiver.
Virtual Circuit	Les valeurs **Virtual Path Identifier (VPI)** et **Virtual Channel Identifier (VCI)** sont utilisées pour identifier votre ligne sur le réseau ATM de votre FAI.
SRA (Seamless Rate Adaptation)	Cochez la case **Enable** ou la case **Disable** pour activer ou désactiver le SRA, un protocole qui, en découplant la modulation et la couche de synchronisation, peut modifier les paramètres de vitesse de transmission des données (appliqués par la couche de modulation).
DSL Modulation	Sélectionnez la modulation DSL dans la liste déroulante. La modulation DSL par défaut est **Multimode** (recommandé).

Dans la section **DSL Settings** du mode de transfert PTM (RV134W), saisissez les informations suivantes :

Mode de transfert	PTM
SRA (Seamless Rate Adaptation)	Cochez la case **Enable** ou la case **Disable** pour activer ou désactiver le SRA, un protocole qui, en découplant la modulation et la couche de synchronisation, peut modifier les paramètres de vitesse de transmission des données (appliqués par la couche de modulation).
DSL Modulation	Sélectionnez la modulation DSL dans la liste déroulante. La modulation DSL par défaut est **Multimode** (recommandé).

Dans la section **PPPoE Settings** des modes de transfert ATM et PTM (RV134W), saisissez les informations suivantes :

Username	Saisissez le nom d'utilisateur.
Password	Saisissez le mot de passe.
DNS Server Source	Sélectionnez **Get Dynamically from ISP** ou **Use These DNS Servers** pour configurer les paramètres manuellement.
Static DNS 1 et 2	Saisissez l'adresse IP du serveur DNS statique principal et/ou secondaire dans les champs (conseil 1.2.3.4).
Connect on Demand Max Idle Time	Sélectionnez cette option si votre FAI vous fait payer dès que vous êtes connecté à Internet. Si vous sélectionnez cette option, la connexion Internet n'est activée qu'en présence d'un trafic. Si la connexion est en attente (sans trafic en transit), elle est fermée. Si vous cochez la case Connect on Demand, saisissez le délai (en minutes) avant déconnexion dans le champ Max Idle Time.

Keep Alive	Lorsque vous sélectionnez cette option, la connexion Internet est toujours active. Dans le champ **Redial Period**, saisissez le délai en secondes à l'issue duquel l'appareil, s'il est déconnecté, tente de se reconnecter.
Authentication Type	Sélectionnez le type d'authentification dans la liste déroulante. **Auto Negotiation** : le serveur envoie une requête de configuration spécifiant l'algorithme de sécurité paramétré. L'appareil renvoie alors les identifiants d'authentification avec le type de sécurité envoyé par le serveur. **PAP** : protocole d'authentification du mot de passe. **CHAP** : Challenge Handshake Authentication Protocol. **MS-CHAP** : version Microsoft du protocole CHAP (Challenge-Handshake Authentication Protocol). **MS-CHAP2** : version Microsoft du protocole Challenge-Handshake Authentication Protocol version 2.
Service Name	Saisissez le nom du service.

Dans la section **IPv6 Settings** des modes de transfert ATM et PTM (RV134W), saisissez les informations suivantes **:**

Pour IPv6

Mode	IPv6
Address Mode	Sélectionnez **Dynamic** ou **Static**. Si vous sélectionnez **Dynamic** et que le message RA (Annonce de routeur) reçu par le périphérique contient une balise M « 0 », le périphérique utilise SLAAC (Stateless Address Auto-configuration) pour obtenir les adresses IPv6 ; si la balise M est « 1 », il utilise DHCPv6 pour obtenir l'adresse IPv6. Si vous sélectionnez **Static**, saisissez les informations suivantes : ▪ IPv6 Address ▪ IPv6 Prefix Length ▪ Default IPv6 Gateway ▪ IPv6 DNS1 et DNS2 La connexion IPv6 est également PPPoE. Les connexions IPv4 et IPv6 partagent le même paramètre PPPoE.
Prefix Delegation	Pour affecter un préfixe d'adresse réseau (du FAI) au réseau LAN, activez l'option **Prefix Delegation**.

Pour 6rd

Mode	6rd
6rd Tunneling	Sélectionnez **Auto** ou **Manual**. Si vous sélectionnez **Manual**, saisissez les informations suivantes : ▪ IPv6 Prefix ▪ IPv6 Prefix Length ▪ Border Relay ▪ IPv4 Mask Length

Dans la section **Other Settings** des modes de transfert ATM et PTM (RV134W), saisissez les informations suivantes **:**

NAT (Network Address Translation)	Si cette option est activée, tout le trafic sortant par le biais de cette interface est traduit en adresses réseau (NAT). Si elle est désactivée, tout le trafic sortant par le biais de cette interface est acheminé.
VLAN et VLAN ID	Si cette option est activée, tout le trafic sortant par le biais de cette interface est balisé avec l'ID VLAN configuré**.**
Reset Timer	Pour PPPoE uniquement : Réinitialisez la connexion PPPoE à une heure et un jour donnés de la semaine. Choisissez l'une des options suivantes dans la liste déroulante **Frequency** et spécifiez les paramètres correspondants : **Never** : choisissez cette option pour désactiver cette fonction. **Daily** : choisissez cette option pour réinitialiser la connexion PPPoE à une heure donnée de la journée. Saisissez l'heure de la journée dans le champ Time. **Weekly** : choisissez cette option pour réinitialiser la connexion PPPoE à un jour donné de la semaine. Saisissez ensuite le jour de la semaine et l'heure de la journée
MTU (Maximum Transmission Unit)	MTU est une configuration avancée qui vous permet de déterminer la taille de données maximale autorisée sur votre connexion. Sélectionnez **Auto** (valeur par défaut) ou **Manual** pour configurer les paramètres manuellement.
Size	Saisissez la taille en octets (Plage : 576 - 1492, valeur par défaut : 1492).

MAC Address Clone	Il peut arriver que vous deviez définir l'adresse MAC du port WAN du périphérique afin qu'il ait la même adresse que votre ordinateur ou une autre adresse MAC. C'est ce que l'on appelle cloner l'adresse MAC. Par exemple, certains FAI enregistrent l'adresse MAC de la carte de votre ordinateur lors de l'installation initiale du service. Si vous installez ensuite un routeur derrière le modem câble ou DSL, l'adresse MAC du port WAN du périphérique n'est pas reconnue par le FAI. Pour configurer votre périphérique afin qu'il soit reconnu par le FAI, vous pouvez alors cloner l'adresse MAC du port WAN afin qu'elle soit identique à celle de votre ordinateur. Pour configurer un clone d'adresse MAC, sélectionnez **Enable.**
MAC Address	Pour définir l'adresse MAC du port WAN de l'appareil, effectuez l'une des opérations suivantes : Pour définir l'adresse MAC du port WAN sur l'adresse MAC de votre PC, cliquez sur **Clone My PC's MAC**. Pour spécifier une autre adresse MAC, saisissez-la dans le champ **MAC Address**.

Lorsque le type de connexion Internet est PPPoA :

Dans la section **DSL Settings**, saisissez les informations suivantes :

Mode de transfert	ATM
Multiplexing	Définit la manière dont différents protocoles sont gérés dans un circuit virtuel DSL. Vous pouvez choisir entre une encapsulation LLC (Logical Link Control) et le multiplexage VC (Virtual Channel).

QoS Type	Sélectionnez la qualité de service (QoS) DSL : Unspecified Bit Rate (UBR), Constant Bit Rate (CBR), Variable Bit Rate - real time (VBR-rt), Variable Bit Rate - non-real time (VBR-nrt). CBR offre la meilleure garantie de faible latence : UBR n'en fournit aucune, mais est généralement utilisé pour la plupart des services de données haut débit. **Pcr Rate** : lorsque la qualité de service est définie sur CBR, VBR-rt ou VBR-nrt, saisissez le débit de cellules crête (PCR) en cellules par seconde. **Scr Rate** : lorsque la qualité de service est définie sur VBR-rt ou VBR-nrt, saisissez le taux de cellules retenu (SCR) en cellules par seconde.
Auto Detect	Cochez la case **Enable** pour activer la détection automatique des valeurs VPI et VCI qui identifient votre ligne sur le réseau ATM, ou la case **Disable** pour la désactiver.
Virtual Circuit	Les valeurs **Virtual Path Identifier (VPI)** et **Virtual Channel Identifier (VCI)** sont utilisées pour identifier votre ligne sur le réseau ATM de votre FAI.
SRA (Seamless Rate Adaptation)	Cochez la case **Enable** ou la case **Disable** pour activer ou désactiver le SRA, un protocole qui, en découplant la modulation et la couche de synchronisation, peut modifier les paramètres de vitesse de transmission des données (appliqués par la couche de modulation).
DSL Modulation	Sélectionnez la modulation DSL dans la liste déroulante. La modulation DSL par défaut est **Multimode** (recommandé).

Dans la section **PPPoA Settings**, saisissez les informations suivantes :

Username	Saisissez le nom d'utilisateur.
Password	Saisissez le mot de passe.
DNS Server Source	Sélectionnez **Get Dynamically from ISP** ou **Use These DNS Servers** pour configurer les paramètres manuellement.

Static DNS 1 et 2	Saisissez l'adresse IP du serveur DNS statique principal et/ou secondaire dans les champs (conseil 1.2.3.4).
Connect on Demand Max Idle Time	Sélectionnez cette option si votre FAI vous facture en fonction de la durée de connexion. Lorsque vous sélectionnez cette option, la connexion Internet n'est activée qu'en présence d'un trafic. Si la connexion est en attente (sans trafic en transit), elle est fermée. Si vous cochez la case Connect on Demand, saisissez le délai (en minutes) avant déconnexion dans le champ Max Idle Time.
Keep Alive	Lorsque vous sélectionnez cette option, la connexion Internet est toujours active. Dans le champ **Redial Period**, saisissez le délai en secondes à l'issue duquel l'appareil, s'il est déconnecté, tente de se reconnecter.
Authentication Type	Sélectionnez le type d'authentification dans la liste déroulante. **Auto Negotiation** : le serveur envoie une requête de configuration spécifiant l'algorithme de sécurité paramétré. L'appareil renvoie alors les identifiants d'authentification avec le type de sécurité envoyé par le serveur. **PAP** : protocole d'authentification du mot de passe. **CHAP** : Challenge Handshake Authentication Protocol. **MS-CHAP** : version Microsoft du protocole CHAP (Challenge-Handshake Authentication Protocol). **MS-CHAP2** : version Microsoft du protocole Challenge-Handshake Authentication Protocol version 2.

Dans la section **IPv6 Settings**, saisissez les informations suivantes :

Pour IPv6

Mode	IPv6
Address Mode	Sélectionnez **Dynamic** ou **Static**. Si vous sélectionnez **Dynamic** et que le message RA (Annonce de routeur) reçu par le périphérique contient une balise M « 0 », le périphérique utilise SLAAC (Stateless Address Auto-configuration) pour obtenir les adresses IPv6 ; si la balise M est « 1 », il utilise DHCPv6 pour obtenir l'adresse IPv6. Si vous sélectionnez **Static**, saisissez les informations suivantes : ▪ IPv6 Address ▪ IPv6 Prefix Length ▪ Default IPv6 Gateway ▪ IPv6 DNS1 et DNS2 La connexion IPv6 est également PPPoA. Les connexions IPv4 et IPv6 partagent le même paramètre PPPoA.
Prefix Delegation	Pour affecter un préfixe d'adresse réseau (du FAI) au réseau LAN, activez l'option **Prefix Delegation**.

Pour 6rd

Mode	6rd
6rd Tunneling	Sélectionnez **Auto** ou **Manual**. Si vous sélectionnez **Manual**, saisissez les informations suivantes : ▪ IPv6 Prefix ▪ IPv6 Prefix Length ▪ Border Relay ▪ IPv4 Mask Length

Dans la section **Other Settings**, saisissez les informations suivantes :

NAT (Network Address Translation)	Si cette option est activée, tout le trafic sortant par le biais de cette interface est traduit en adresses réseau (NAT). Si elle est désactivée, tout le trafic sortant par le biais de cette interface est acheminé.
MTU (Maximum Transmission Unit)	MTU est une configuration avancée qui vous permet de déterminer la taille de données maximale autorisée sur votre connexion. Sélectionnez **Auto** (valeur par défaut) ou **Manual** pour configurer les paramètres manuellement.
Size	Saisissez la taille en octets (Plage : 576 - 1 492, valeur par défaut : 1 492).
MAC Address Clone	Il peut arriver que vous deviez définir l'adresse MAC du port WAN du périphérique afin qu'il ait la même adresse que votre ordinateur ou une autre adresse MAC. C'est ce que l'on appelle cloner l'adresse MAC. Par exemple, certains FAI enregistrent l'adresse MAC de la carte de votre ordinateur lors de l'installation initiale du service. Si vous installez ensuite un routeur derrière le modem câble ou DSL, l'adresse MAC du port WAN du périphérique n'est pas reconnue par le FAI. Pour configurer votre périphérique afin qu'il soit reconnu par le FAI, vous pouvez alors cloner l'adresse MAC du port WAN afin qu'elle soit identique à celle de votre ordinateur. Pour configurer un clone d'adresse MAC, sélectionnez **Enable.**
MAC Address	Pour définir l'adresse MAC du port WAN du périphérique, effectuez l'une des opérations suivantes : Pour définir l'adresse MAC du port WAN sur l'adresse MAC de votre PC, cliquez sur **Clone My PC's MAC**. Pour spécifier une autre adresse MAC, saisissez-la dans le champ **MAC Address**.

Configuration du réseau WAN Ethernet

Lorsque le type de connexion est DHCP :

Dans la section **DCHP Settings**, saisissez les informations suivantes :

DNS Server Source	Sélectionnez **Get Dynamically from ISP** ou **Use These DNS Servers** pour configurer les paramètres manuellement.
Static DNS1 et 2	Saisissez l'adresse IP du serveur DNS statique principal et/ou secondaire dans les champs (conseil 1.2.3.4).

Dans la section **IPv6 Settings**, saisissez les informations suivantes :

Pour IPv6

Mode	IPv6
Address Mode	Sélectionnez **Dynamic** ou **Static**. Si vous sélectionnez **Dynamic** et que le message RA (Annonce de routeur) reçu par le périphérique contient une balise M « 0 », le périphérique utilise SLAAC (Stateless Address Auto-configuration) pour obtenir les adresses IPv6 ; si la balise M est « 1 », il utilise DHCPv6 pour obtenir l'adresse IPv6. Si vous sélectionnez **Static**, saisissez les informations suivantes : ▪ IPv6 Address ▪ IPv6 Prefix Length ▪ Default IPv6 Gateway ▪ IPv6 DNS1 et DNS2
Prefix Delegation	Pour affecter un préfixe d'adresse réseau (du FAI) au réseau LAN, activez l'option **Prefix Delegation**.

Pour 6rd

Mode	6rd
6rd Tunneling	Sélectionnez **Auto** ou **Manual**. Si vous sélectionnez **Manual**, saisissez les informations suivantes : ▪ IPv6 Prefix ▪ IPv6 Prefix Length ▪ Border Relay ▪ IPv4 Mask Length

Dans la section **Other Settings**, saisissez les informations suivantes **:**

NAT (Network Address Translation)	Si cette option est activée, tout le trafic sortant par le biais de cette interface est traduit en adresses réseau (NAT). Si elle est désactivée, tout le trafic sortant par le biais de cette interface est acheminé.
MTU (Maximum Transmission Unit)	MTU est une configuration avancée qui vous permet de déterminer la taille de données maximale autorisée sur votre connexion. Sélectionnez **Auto** (valeur par défaut) ou **Manual** pour configurer les paramètres manuellement.
Size	Saisissez la taille en octets (Plage : 576 - 1 500, valeur par défaut : 1 500).

MAC Address Clone	Il peut arriver que vous deviez définir l'adresse MAC du port WAN du périphérique afin qu'il ait la même adresse que votre ordinateur ou une autre adresse MAC. C'est ce que l'on appelle cloner l'adresse MAC. Par exemple, certains FAI enregistrent l'adresse MAC de la carte de votre ordinateur lors de l'installation initiale du service. Si vous installez ensuite un routeur derrière le modem câble ou DSL, l'adresse MAC du port WAN du périphérique n'est pas reconnue par le FAI. Pour configurer votre périphérique afin qu'il soit reconnu par le FAI, vous pouvez alors cloner l'adresse MAC du port WAN afin qu'elle soit identique à celle de votre ordinateur. Pour configurer un clone d'adresse MAC, sélectionnez **Enable.**
MAC Address	Pour définir l'adresse MAC du port WAN du périphérique, effectuez l'une des opérations suivantes : Pour définir l'adresse MAC du port WAN sur l'adresse MAC de votre PC, cliquez sur **Clone My PC's MAC**. Pour spécifier une autre adresse MAC, saisissez-la dans le champ **MAC Address**.

Lorsque le type de connexion Internet est IP statique :

Dans la section **Static IP** Settings, saisissez les informations suivantes **:**

Internet IP Address	Adresse IP du port WAN.
Subnet mask	Masque de sous-réseau du port WAN.
Default Gateway	Adresse IP de la passerelle par défaut.
Static DNS1 et 2	Saisissez l'adresse IP du serveur DNS statique principal et/ou secondaire dans les champs (conseil 1.2.3.4).

Dans la section **IPv6 Settings**, saisissez les informations suivantes :

Pour IPv6

Mode	IPv6
Address Mode	Sélectionnez **Dynamic** ou **Static**. Si vous sélectionnez **Dynamic** et que le message RA (Annonce de routeur) reçu par le périphérique contient une balise M « 0 », le périphérique utilise SLAAC (Stateless Address Auto-configuration) pour obtenir les adresses IPv6 ; si la balise M est « 1 », il utilise DHCPv6 pour obtenir l'adresse IPv6. Si vous sélectionnez **Static**, saisissez les informations suivantes : ▪ IPv6 Address ▪ IPv6 Prefix Length ▪ Default IPv6 Gateway ▪ IPv6 DNS1 et DNS2
Prefix Delegation	Pour affecter un préfixe d'adresse réseau (du FAI) au réseau LAN, activez l'option **Prefix Delegation**.

Pour 6rd

Mode	6rd
6rd Tunneling	Sélectionnez **Auto** ou **Manual**. Si vous sélectionnez **Manual**, saisissez les informations suivantes : ▪ IPv6 Prefix ▪ IPv6 Prefix Length ▪ Border Relay ▪ IPv4 Mask Length

Dans la section **Other Settings**, saisissez les informations suivantes :

NAT (Network Address Translation)	Si cette option est activée, tout le trafic sortant par le biais de cette interface est traduit en adresses réseau (NAT). Si elle est désactivée, tout le trafic sortant par le biais de cette interface est acheminé.
VLAN et VLAN ID	Si cette option est activée, tout le trafic sortant par le biais de cette interface est balisé avec l'ID VLAN configuré.
802.1p Priority	Saisissez une plage entre 0 et 7. Tout le trafic sortant de cette interface est balisé avec la priorité 802.1p configurée. S'il entre en conflit avec le paramètre QoS, celui-ci est prioritaire.
MTU (Maximum Transmission Unit)	MTU est une configuration avancée qui vous permet de déterminer la taille de données maximale autorisée sur votre connexion. Sélectionnez **Auto** (valeur par défaut) ou **Manual** pour configurer les paramètres manuellement.
Size	Saisissez la taille en octets (Plage : 576 - 1 500, valeur par défaut : 1 500).
MAC Address Clone	Il peut arriver que vous deviez définir l'adresse MAC du port WAN du périphérique afin qu'il ait la même adresse que votre ordinateur ou une autre adresse MAC. C'est ce que l'on appelle cloner l'adresse MAC. Par exemple, certains FAI enregistrent l'adresse MAC de la carte de votre ordinateur lors de l'installation initiale du service. Si vous installez ensuite un routeur derrière le modem câble ou DSL, l'adresse MAC du port WAN du périphérique n'est pas reconnue par le FAI. Pour configurer votre périphérique afin qu'il soit reconnu par le FAI, vous pouvez alors cloner l'adresse MAC du port WAN afin qu'elle soit identique à celle de votre ordinateur. Pour configurer un clone d'adresse MAC, sélectionnez **Enable.**

MAC Address	Pour définir l'adresse MAC du port WAN du périphérique, effectuez l'une des opérations suivantes : Pour définir l'adresse MAC du port WAN sur l'adresse MAC de votre PC, cliquez sur **Clone My PC's MAC**. Pour spécifier une autre adresse MAC, saisissez-la dans le champ **MAC Address**.

Lorsque le type de connexion Internet est PPPoE :

Dans la section **PPPoE Settings**, saisissez les informations suivantes **:**

Username	Saisissez le nom d'utilisateur.
Password	Saisissez le mot de passe.
DNS Server Source	Sélectionnez **Get Dynamically from ISP** ou **Use These DNS Servers** pour configurer les paramètres manuellement.
Static DNS 1 et 2	Saisissez l'adresse IP du serveur DNS statique principal et/ou secondaire dans les champs (conseil 1.2.3.4).
Connect on Demand Max Idle Time	Sélectionnez cette option si votre FAI vous fait payer dès que vous êtes connecté à Internet. Si vous sélectionnez cette option, la connexion Internet n'est activée qu'en présence d'un trafic. Si la connexion est en attente (sans trafic en transit), elle est fermée. Si vous cochez la case Connect on Demand, saisissez le délai (en minutes) avant déconnexion dans le champ Max Idle Time.
Keep Alive	Lorsque vous sélectionnez cette option, la connexion Internet est toujours active. Dans le champ **Redial Period**, saisissez le délai en secondes à l'issue duquel le périphérique, s'il est déconnecté, tente de se reconnecter.

Authentication Type	Sélectionnez le type d'authentification dans la liste déroulante. **Auto Negotiation** : le serveur envoie une requête de configuration spécifiant l'algorithme de sécurité paramétré. Le périphérique renvoie alors les identifiants d'authentification avec le type de sécurité envoyé par le serveur. **PAP** : protocole d'authentification du mot de passe. **CHAP** : Challenge Handshake Authentication Protocol. **MS-CHAP** : version Microsoft du protocole CHAP (Challenge-Handshake Authentication Protocol). **MS-CHAP2** : version Microsoft du protocole Challenge-Handshake Authentication Protocol version 2.
Service Name	Saisissez le nom du service.

Dans la section **IPv6 Settings**, saisissez les informations suivantes :

Pour IPv6

Mode	IPv6
Address Mode	Sélectionnez **Dynamic** ou **Static**. Si vous sélectionnez **Dynamic** et que le message RA (Annonce de routeur) reçu par le périphérique contient une balise M « 0 », le périphérique utilise SLAAC (Stateless Address Auto-configuration) pour obtenir les adresses IPv6 ; si la balise M est « 1 », il utilise DHCPv6 pour obtenir l'adresse IPv6. Si vous sélectionnez **Static**, saisissez les informations suivantes : ▪ IPv6 Address ▪ IPv6 Prefix Length ▪ Default IPv6 Gateway ▪ IPv6 DNS1 et DNS2 La connexion IPv6 est également PPPoE. Les connexions IPv4 et IPv6 partagent le même paramètre PPPoE.
Prefix Delegation	Pour affecter un préfixe d'adresse réseau (du FAI) au réseau LAN, activez l'option **Prefix Delegation**.

Pour 6rd

Mode	6rd
6rd Tunneling	Sélectionnez **Auto** ou **Manual**. Si vous sélectionnez **Manual**, saisissez les informations suivantes : ▪ IPv6 Prefix ▪ IPv6 Prefix Length ▪ Border Relay ▪ IPv4 Mask Length

Dans la section **Other Settings**, saisissez les informations suivantes :

NAT (Network Address Translation)	Si cette option est activée, tout le trafic sortant par le biais de cette interface est traduit en adresses réseau (NAT). Si elle est désactivée, tout le trafic sortant par le biais de cette interface est acheminé.
VLAN et VLAN ID	Si cette option est activée, tout le trafic sortant par le biais de cette interface est balisé avec l'ID VLAN configuré**.**
802.1p Priority	Saisissez une plage entre 0 et 7. Tout le trafic sortant de cette interface est balisé avec la priorité 802.1p configurée. S'il entre en conflit avec le paramètre QoS, celui-ci est prioritaire.
Reset Timer	Pour PPPoE uniquement : Réinitialisez la connexion PPPoE à une heure et un jour donnés de la semaine. Choisissez l'une des options suivantes dans la liste déroulante **Frequency** et spécifiez les paramètres correspondants : **Never** : choisissez cette option pour désactiver cette fonction. **Daily** : choisissez cette option pour réinitialiser la connexion PPPoE à une heure donnée de la journée. Saisissez l'heure de la journée dans le champ Time. **Weekly** : choisissez cette option pour réinitialiser la connexion PPPoE à un jour donné de la semaine. Saisissez ensuite le jour de la semaine et l'heure de la journée.
MTU (Maximum Transmission Unit)	MTU est une configuration avancée qui vous permet de déterminer la taille de données maximale autorisée sur votre connexion. Sélectionnez **Auto** (valeur par défaut) ou **Manual** pour configurer les paramètres manuellement.
Size	Saisissez la taille en octets (Plage : 576 - 1 492, valeur par défaut : 1 492).

MAC Address Clone	Il peut arriver que vous deviez définir l'adresse MAC du port WAN du périphérique afin qu'il ait la même adresse que votre ordinateur ou une autre adresse MAC. C'est ce que l'on appelle cloner l'adresse MAC. Par exemple, certains FAI enregistrent l'adresse MAC de la carte de votre ordinateur lors de l'installation initiale du service. Si vous installez ensuite un routeur derrière le modem câble ou DSL, l'adresse MAC du port WAN du périphérique n'est pas reconnue par le FAI. Pour configurer votre périphérique afin qu'il soit reconnu par le FAI, vous pouvez alors cloner l'adresse MAC du port WAN afin qu'elle soit identique à celle de votre ordinateur. Pour configurer un clone d'adresse MAC, sélectionnez **Enable.**
MAC Address	Pour définir l'adresse MAC du port WAN du périphérique, effectuez l'une des opérations suivantes : Pour définir l'adresse MAC du port WAN sur l'adresse MAC de votre PC, cliquez sur **Clone My PC's MAC**. Pour spécifier une autre adresse MAC, saisissez-la dans le champ **MAC Address**.

Lorsque le type de connexion Internet est L2TP (RV134W) :

Dans la section **L2TP Settings**, saisissez les informations suivantes :

Auto Get IP (DHCP)	Cochez la case **Enable** ou la case **Disable** pour activer ou désactiver le paramètre Auto get IP (DHCP), une méthode d'affectation automatique des adresses IP. S'il est désactivé, configurez manuellement l'adresse IP.
L2TP Server	Saisissez l'adresse IP (conseil 192.168.1.10).
Username	Saisissez le nom d'utilisateur.
Password	Saisissez le mot de passe.
DNS Server Source	Sélectionnez **Get Dynamically from ISP** ou **Use These DNS Servers** pour configurer les paramètres manuellement.

Static DNS 1 et 2	Saisissez l'adresse IP du serveur DNS statique principal et/ou secondaire dans les champs (conseil 1.2.3.4).
Connect on Demand Max Idle Time	Sélectionnez cette option si votre FAI vous fait payer dès que vous êtes connecté. Lorsque vous sélectionnez cette option, la connexion Internet n'est activée qu'en présence d'un trafic. Si la connexion est en attente (sans trafic en transit), elle est fermée. Si vous cliquez sur Connect on Demand, saisissez le délai (en minutes) avant déconnexion dans le champ Max Idle Time.
Keep Alive	Lorsque vous sélectionnez cette option, la connexion Internet est toujours active. Dans le champ **Redial Period**, saisissez le délai en secondes à l'issue duquel le périphérique, s'il est déconnecté, tente de se reconnecter.

Dans la section **IPv6 Settings**, saisissez les informations suivantes :

Pour IPv6

Mode	IPv6
Address Mode	Sélectionnez **Dynamic** ou **Static**. Si vous sélectionnez **Dynamic** et que le message RA (Annonce de routeur) reçu par le périphérique contient une balise M « 0 », le périphérique utilise SLAAC (Stateless Address Auto-configuration) pour obtenir les adresses IPv6 ; si la balise M est « 1 », il utilise DHCPv6 pour obtenir l'adresse IPv6. Si vous sélectionnez **Static**, saisissez les informations suivantes : ▪ IPv6 Address ▪ IPv6 Prefix Length ▪ Default IPv6 Gateway ▪ IPv6 DNS1 et DNS2
Prefix Delegation	Pour affecter un préfixe d'adresse réseau (du FAI) au réseau LAN, activez l'option **Prefix Delegation**.

Pour 6rd

Mode	6rd
6rd Tunneling	Sélectionnez **Auto** ou **Manual**. Si vous sélectionnez **Manual**, saisissez les informations suivantes : ▪ IPv6 Prefix ▪ IPv6 Prefix Length ▪ Border Relay ▪ IPv4 Mask Length

Dans la section **Other Settings**, saisissez les informations suivantes :

NAT (Network Address Translation)	Si cette option est activée, tout le trafic sortant par le biais de cette interface est traduit en adresses réseau (NAT). Si elle est désactivée, tout le trafic sortant par le biais de cette interface est acheminé.
VLAN et VLAN ID	Si cette option est activée, tout le trafic sortant par le biais de cette interface est balisé avec l'ID VLAN configuré**.**
802.1p Priority	Saisissez une plage entre 0 et 7. Tout le trafic sortant de cette interface est balisé avec la priorité 802.1p configurée. S'il entre en conflit avec le paramètre QoS, celui-ci est prioritaire.
MTU (Maximum Transmission Unit)	MTU est une configuration avancée qui vous permet de déterminer la taille de données maximale autorisée sur votre connexion. Sélectionnez **Auto** (valeur par défaut) ou **Manual** pour configurer les paramètres manuellement.
Size	Saisissez la taille en octets (Plage : 576 - 1 460, valeur par défaut : 1 460).

MAC Address Clone	Il peut arriver que vous deviez définir l'adresse MAC du port WAN du périphérique afin qu'il ait la même adresse que votre ordinateur ou une autre adresse MAC. C'est ce que l'on appelle cloner l'adresse MAC. Par exemple, certains FAI enregistrent l'adresse MAC de la carte de votre ordinateur lors de l'installation initiale du service. Si vous installez ensuite un routeur derrière le modem câble ou DSL, l'adresse MAC du port WAN du périphérique n'est pas reconnue par le FAI. Pour configurer votre périphérique afin qu'il soit reconnu par le FAI, vous pouvez alors cloner l'adresse MAC du port WAN afin qu'elle soit identique à celle de votre ordinateur. Pour configurer un clone d'adresse MAC, sélectionnez **Enable.**
MAC Address	Pour définir l'adresse MAC du port WAN du périphérique, effectuez l'une des opérations suivantes : Pour définir l'adresse MAC du port WAN sur l'adresse MAC de votre PC, cliquez sur **Clone My PC's MAC**. Pour spécifier une autre adresse MAC, saisissez-la dans le champ **MAC Address**.

Lorsque le type de connexion Internet est PPTP :

Dans la section **PPTP Setting**, saisissez les informations suivantes :

Auto Get IP (DHCP)	Cochez la case **Enable** ou la case **Disable** pour activer ou désactiver le paramètre Auto get IP (DHCP), une méthode d'affectation automatique des adresses IP. S'il est désactivé, configurez manuellement l'adresse IP.
PPTP Server Type	Sélectionnez **IP Address** ou **FQDN.**
PPTP Server	Adresse IP du serveur PPTP (Point-To-Point Tunneling Protocol).
Username	Nom d'utilisateur qui vous est affecté par le FAI.

Password	Mot de passe qui vous est affecté par le FAI.
DNS Server Source	Adresse du serveur DNS. Si vous avez déjà reçu les adresses de serveur DNS de votre FAI, choisissez **Use these DNS Servers**, puis saisissez les adresses principale et secondaire dans les champs **Static DNS 1** et **Static DNS 2**. Pour recevoir les adresses de serveur DNS de votre FAI, choisissez **Get Dynamically from ISP**.
Connect on Demand	Sélectionnez cette option si votre FAI vous facture en fonction de la durée de connexion. Lorsque vous sélectionnez cette option, la connexion Internet n'est activée qu'en présence d'un trafic. Si la connexion est en attente (sans trafic en transit), elle est fermée. Si vous cochez **Connect on Demand**, saisissez délai (en minutes) avant déconnexion dans le champ **Max Idle Time**.
Keep Alive	Lorsque vous sélectionnez cette option, la connexion Internet est toujours active. Dans le champ **Redial Period**, saisissez le délai en secondes à l'issue duquel le périphérique, s'il est déconnecté, tente de se reconnecter.
Authentication Type	Sélectionnez le type d'authentification : **Auto-negotiation** : le serveur envoie une requête de configuration spécifiant l'algorithme de sécurité paramétré. Le périphérique renvoie alors les identifiants d'authentification avec le type de sécurité précédemment envoyé par le serveur. **PAP** : le périphérique utilise le protocole PAP (Password Authentication Protocol) lors de la connexion au FAI. **CHAP** : le périphérique utilise le protocole CHAP (Challenge Handshake Authentication Protocol) lors de la connexion au FAI. **MS-CHAP ou MS-CHAPv2** : le périphérique utilise le protocole MS-CHAP (Microsoft Challenge Handshake Authentication Protocol) lors de la connexion au FAI.

MPPE Encryption	MPPE (Microsoft Point-to-Point Encryption) crypte les données dans les connexions d'accès à distance PPP (Point-to-Point Protocol) ou les connexions via un réseau privé virtuel (VPN) PPTP (Point-to-Point Tunneling Protocol). Cochez la case **Enable** pour activer le cryptage MPPE.

Dans la section **IPv6 Settings**, saisissez les informations suivantes :

Pour IPv6

Mode	IPv6
Address Mode	Sélectionnez **Dynamic** ou **Static**. Si vous sélectionnez **Dynamic** et que le message RA (Annonce de routeur) reçu par le périphérique contient une balise M « 0 », le périphérique utilise SLAAC (Stateless Address Auto-configuration) pour obtenir les adresses IPv6 ; si la balise M est « 1 », il utilise DHCPv6 pour obtenir l'adresse IPv6. Si vous sélectionnez **Static**, saisissez les informations suivantes : ▪ IPv6 Address ▪ IPv6 Prefix Length ▪ Default IPv6 Gateway ▪ IPv6 DNS1 et DNS2
Prefix Delegation	Pour affecter un préfixe d'adresse réseau (du FAI) au réseau LAN, activez l'option **Prefix Delegation**.

Pour 6rd

Mode	6rd
6rd Tunneling	Sélectionnez **Auto** ou **Manual**. Si vous sélectionnez **Manual**, saisissez les informations suivantes : ▪ IPv6 Prefix ▪ IPv6 Prefix Length ▪ Border Relay ▪ IPv4 Mask Length

Dans la section **Other Settings**, saisissez les informations suivantes :

NAT (Network Address Translation)	Si cette option est activée, tout le trafic sortant par le biais de cette interface est traduit en adresses réseau (NAT). Si elle est désactivée, tout le trafic sortant par le biais de cette interface est acheminé.
VLAN et VLAN ID	Si cette option est activée, tout le trafic sortant par le biais de cette interface est balisé avec l'ID VLAN configuré**.**
802.1p Priority	Saisissez une plage entre 0 et 7. Tout le trafic sortant de cette interface est balisé avec la priorité 802.1p configurée. S'il entre en conflit avec le paramètre QoS, celui-ci est prioritaire.
MTU (Maximum Transmission Unit)	MTU est une configuration avancée qui vous permet de déterminer la taille de données maximale autorisée sur votre connexion. Sélectionnez **Auto** (valeur par défaut) ou **Manual** pour configurer les paramètres manuellement.
Size	Saisissez la taille en octets (Plage : 576 - 1 460, valeur par défaut : 1 460).

MAC Address Clone	Il peut arriver que vous deviez définir l'adresse MAC du port WAN du périphérique afin qu'il ait la même adresse que votre ordinateur ou une autre adresse MAC. C'est ce que l'on appelle cloner l'adresse MAC. Par exemple, certains FAI enregistrent l'adresse MAC de la carte de votre ordinateur lors de l'installation initiale du service. Si vous installez ensuite un routeur derrière le modem câble ou DSL, l'adresse MAC du port WAN du périphérique n'est pas reconnue par le FAI. Pour configurer votre périphérique afin qu'il soit reconnu par le FAI, vous pouvez alors cloner l'adresse MAC du port WAN afin qu'elle soit identique à celle de votre ordinateur. Pour configurer un clone d'adresse MAC, sélectionnez **Enable.**
MAC Address	Pour définir l'adresse MAC du port WAN du périphérique, effectuez l'une des opérations suivantes : Pour définir l'adresse MAC du port WAN sur l'adresse MAC de votre PC, cliquez sur **Clone My PC's MAC**. Pour spécifier une autre adresse MAC, saisissez-la dans le champ **MAC Address**.

Configuration d'un réseau mobile

Sélectionnez **Networking > WAN > Mobile Network** pour configurer le périphérique en vue de sa connexion à un modem USB haut débit mobile, qui est lui-même connecté à son interface USB.

Configuration des paramètres de réseau mobile globaux

Pour configurer les paramètres globaux des périphériques USB pris en charge :

ÉTAPE 1 Connectez le modem USB. Si le modem est pris en charge, il est détecté automatiquement et apparaît sur la page Mobile Network.

ÉTAPE 2 Sélectionnez le mode de connexion **Auto** ou **Manual**. La récupération de la connexion Ethernet fonctionne uniquement si le mode de connexion est défini sur Auto.

- Pour permettre à votre modem d'établir une connexion automatiquement, sélectionnez le mode **Auto**. Si vous sélectionnez **Auto**, définissez une heure de **Connexion à la demande** ou sélectionnez **Keep Alive**. L'option **Connect on Demand** met fin à la connexion Internet à l'issue de la durée d'inactivité spécifiée dans le champ **Max Idle Time**.
- Si votre connexion Internet est interrompue après une période d'inactivité, le modem établit automatiquement une nouvelle connexion lorsqu'un utilisateur tente d'accéder à Internet. Dans le champ **Max Idle Time**, saisissez le nombre de minutes d'inactivité pouvant s'écouler avant que votre connexion Internet ne soit interrompue. Sélectionnez **Keep Alive** pour maintenir la connexion active en permanence.
- Pour connecter ou déconnecter votre connexion modem manuellement, sélectionnez le mode **Manual**.

Le périphérique affiche l'état actuel de la connexion modem, à savoir Initialisation en cours, Connexion, Déconnexion en cours ou Déconnecté.

ÉTAPE 3 Vérifiez que le champ **Card Status** indique **Connected** pour votre carte mobile.

Configuration manuelle des paramètres de réseau mobile

Pour modifier les paramètres de réseau mobile dans la zone **Mobile Network Setup**, sélectionnez la case d'option **Manual**. Le périphérique détecte automatiquement les modems pris en charge et dresse la liste des paramètres de configuration appropriés. Pour remplacer les paramètres globaux, sélectionnez **Manual**.

ÉTAPE 1 Renseignez les champs suivants :

Champ	Description
Access Point Name (APN)	Réseau Internet auquel l'appareil mobile a établi une connexion. Saisissez le nom du point d'accès spécifié par votre prestataire de services de réseau mobile. Si vous ne connaissez pas le nom du point d'accès, contactez votre prestataire de services.
Dial Number	Composez le numéro fourni par votre prestataire de services de réseau mobile pour accéder à Internet.
Username Password	Nom d'utilisateur et mot de passe spécifiés par votre prestataire de services de réseau mobile.

Champ	Description
SIM PIN	Code PIN associé à votre carte SIM. Ce champ s'affiche uniquement pour les cartes SIM GSM. Vous pouvez modifier le code PIN de la carte SIM en mode Auto ou Manual.
Server Name	Nom du serveur pour la connexion à Internet (s'il est fourni par votre prestataire de services).
Authentication	Authentification utilisée par votre prestataire de services. Cette valeur peut être modifiée en sélectionnant le type d'authentification dans la liste déroulante. La valeur par défaut est **Auto**. Si vous ne connaissez pas le type d'authentification à utiliser, sélectionnez **Auto**.
Server Type	Type de connexion de service de données mobile le plus communément disponible en fonction du signal du service de votre zone. Si votre emplacement prend en charge un seul service de données mobile, vous pouvez limiter l'option de votre choix, en réduisant les durées de configuration de connexion. La première sélection recherche toujours le service HSPDA/3G/UMTS, puis bascule automatiquement vers GPRS, si cette option est disponible.

ÉTAPE 2 Cliquez sur **Save** pour enregistrer vos paramètres.

Paramètre de limite de bande passante

Le périphérique surveille l'activité des données sur la liaison du réseau mobile et lorsqu'il atteint un seuil donné, il envoie une notification.

Pour activer ou désactiver l'option Bandwidth Cap Tracking et définir des limites :

ÉTAPE 1 Cliquez sur **Enabled** ou **Disabled**.

ÉTAPE 2 Sélectionnez **Monthly Renewal Date** dans la liste déroulante afin d'indiquer le jour du mois auquel la limite de bande passante est réinitialisée.

ÉTAPE 3 Dans le champ **Monthly Bandwidth Cap**, saisissez la quantité maximale de données, en méga-octets, pouvant être transmise avant que le routeur ne réagisse, en envoyant, par exemple, un courrier électronique à un administrateur.

Paramètre d'e-mail

Lorsque la limite de données de bande passante est atteinte, un message électronique peut être envoyé à l'administrateur. Pour configurer l'adresse e-mail du destinataire, reportez-vous à la section **Configuration des paramètres d'e-mail**.

- Lorsque cette case est cochée, un courrier électronique est envoyé dans les cas suivants :
- L'utilisation du réseau mobile a dépassé un pourcentage donné.
- Le périphérique bascule sur le mode de secours et une récupération a lieu.
- À chaque intervalle spécifié lorsqu'une liaison du réseau mobile est active.

Configuration du basculement et de la récupération

Si une connexion Ethernet et une liaison du réseau mobile sont disponibles, une seule connexion à la fois peut être utilisée pour établir une liaison WAN. Lorsqu'une connexion WAN échoue, le périphérique essaie d'établir une connexion sur une autre interface. Cette fonctionnalité est connue sous le nom de *basculement.* Lorsque la connexion WAN principale est restaurée, le chemin d'origine est rétabli et la connexion de secours est abandonnée. Cette fonctionnalité est connue sous le nom de *récupération.*

ÉTAPE 1 Sélectionnez **Networking > WAN > Failover & Recovery** pour afficher la fenêtre Failover & Recovery.

ÉTAPE 2 Sélectionnez **Enable Failover to 3G WAN** pour activer la liaison du réseau mobile et la définir pour basculer à partir de la liaison DSL ou Ethernet. Lorsque la liaison WAN Ethernet n'est pas active, le périphérique tente d'activer la liaison du réseau mobile sur l'interface USB (si le basculement n'est pas activé, la liaison du réseau mobile est toujours désactivée).

ÉTAPE 3 Sélectionnez **Enable Recovery back to DSL/Ethernet WAN** pour permettre à la liaison de revenir à la liaison Ethernet, et d'abandonner ainsi la liaison du réseau mobile. Le mode de connexion accessible via **WAN > Mobile Network** doit être défini sur **Auto** pour pouvoir utiliser la récupération de la connexion Ethernet WAN.

ÉTAPE 4 Dans le champ **Failover Check Interval**, saisissez la fréquence (en secondes) à laquelle le périphérique doit tenter de détecter la connexion physique ou la présence de trafic sur la liaison du réseau mobile. Si la liaison est inactive, le périphérique tente d'envoyer une commande ping vers une destination selon cet intervalle. En l'absence de réponse au paquet ping, le périphérique part du principe que la liaison est inactive et retente l'interface Ethernet WAN.

ÉTAPE 5 Dans le champ **Recovery Check Interval**, saisissez la fréquence (en secondes) à laquelle le périphérique doit tenter de détecter la connexion physique ou la présence de trafic sur la liaison WAN Ethernet. Si la liaison est inactive, le périphérique tente d'envoyer une commande ping vers une destination selon cet intervalle. En cas de réponse au paquet ping, le périphérique part du principe que la liaison est active et tente de désactiver la liaison du réseau mobile et d'activer la liaison Ethernet WAN.

ÉTAPE 6 Cliquez sur **Switch back to Ethernet immediately when Ethernet is available** ou sur **Switch back to Ethernet in a specific time range** et saisissez l'heure de début et de fin de la plage.

ÉTAPE 7 Dans le champ **Connection Validation Site**, choisissez le site à partir duquel la validation du basculement doit avoir lieu. Utilisez la passerelle de saut suivant (par défaut, le périphérique envoie une commande ping à la passerelle par défaut) ou choisissez un site personnalisé et saisissez l'adresse IPv4 ou IPv6 de ce site.

ÉTAPE 8 Cliquez sur **Save** pour enregistrer vos paramètres.

La table WAN Interface indique l'état de la liaison Ethernet WAN et de la liaison du réseau mobile sur Internet. Cliquez sur le lien hypertexte **Status** pour afficher les informations relatives au port.

Configuration LAN

Les paramètres DHCP et TCP/IP par défaut sont adaptés à la plupart des applications. Si vous souhaitez qu'un autre ordinateur de votre réseau soit le serveur DHCP, ou si vous souhaitez configurer manuellement les paramètres réseau de tous vos appareils, désactivez DHCP.

Par ailleurs, au lieu d'utiliser un serveur DNS, qui associe les noms de domaines Internet (comme www.cisco.com) à des adresses IP, vous pouvez utiliser un serveur WINS (Windows Internet Naming Service). Un serveur WINS est similaire à un serveur DNS, mais utilise le protocole NetBIOS pour résoudre les noms d'hôte. L'appareil inclut l'adresse IP du serveur WINS dans la configuration DHCP envoyée aux clients DHCP.

Configuration des connexions LAN

L'adresse IP de gestion de périphérique local de l'appareil est statique ; il s'agit de 192.168.1.1 par défaut.

Pour modifier l'adresse IP de gestion de périphérique local :

ÉTAPE 1 Sélectionnez **Networking** > **LAN** > **LAN Configuration**.

ÉTAPE 2 Dans la section Network, saisissez les informations suivantes :

Host Name	Nom d'hôte
Domain Name	Nom de domaine

ÉTAPE 3 Dans la section **IPv4**, saisissez les informations suivantes :

VLAN	Numéro du réseau VLAN.
Local IP Address	Adresse IP LAN locale de l'appareil. Vérifiez que cette adresse IP n'est pas utilisée par un autre appareil.
Subnet mask	Masque de sous-réseau de l'adresse IP locale. La valeur du masque de sous-réseau par défaut est 255.255.255.0.

ÉTAPE 4 Dans le champ **DHCP Server** des paramètres de serveur (DHCP), sélectionnez l'une des options suivantes :

Enable	Permet au périphérique de faire office de serveur DHCP sur le réseau.
Disable	Désactive DHCP sur l'appareil lorsque vous souhaitez configurer manuellement les adresses IP de l'ensemble de vos périphériques réseau.
DHCP Relay	Relaie les adresses IP affectées par un autre serveur DHCP aux périphériques réseau.

Si vous avez activé le serveur DHCP du périphérique, saisissez les informations suivantes :

Default Gateway IP Address	L'adresse IP de passerelle par défaut est l'adresse IP de la passerelle affectée au client DHCP.
Start IP Address	Première adresse du groupe d'adresses IP. Une adresse IP de cette plage est affectée à chaque client DHCP rejoignant le LAN.
End IP Address	Dernière adresse du groupe d'adresses IP. Une adresse IP de cette plage est affectée à chaque client DHCP rejoignant le LAN.
Client Lease time	Durée (en minutes) des baux des adresses IP affectés aux clients.
DNS Server	Sélectionnez le serveur DNS dans la liste déroulante.
Static DNS 1	Adresse IP du serveur DNS principal.
Static DNS 2	Adresse IP du serveur DNS secondaire.
Static DNS 3	Adresse IP du serveur DNS tertiaire.
WINS	Adresse IP du serveur WINS principal.
DHCP Option 66/150 et 67	Cochez la case Enable pour activer l'option DHCP 66/150 et 67.
TFTP Server Host Name	Option 66, nom de l'hôte serveur TFTP.
TFTP Server IP	Option 150, adresse IP du serveur TFTP.
Configuration Filename	Option 67, nom du fichier de configuration.

Si vous avez sélectionné **DHCP Relay**, saisissez l'adresse de la passerelle de relais dans **Remote** Champ **DHCP Server**. La passerelle de relais transmet les messages DHCP entre plusieurs sous-réseaux.

ÉTAPE 5 Cliquez sur **Save**.

Configuration d'une appartenance VLAN

Un LAN virtuel ou VLAN est un groupe de points d'extrémité d'un réseau, associés par fonction ou selon d'autres caractéristiques communes. Contrairement aux LAN, qui se trouvent généralement sur un même site géographique, les VLAN peuvent regrouper des points d'extrémité indépendamment de l'emplacement physique des appareils et des utilisateurs.

Le périphérique comporte un VLAN par défaut (VLAN 1), qui ne peut pas être supprimé. Vous pouvez créer jusqu'à cinq autres VLAN sur le périphérique.

Pour créer un VLAN :

ÉTAPE 1 Sélectionnez **Networking** > **LAN** > **VLAN Membership**.

ÉTAPE 2 Cliquez sur **Add Row**.

ÉTAPE 3 Saisissez les informations suivantes :

VLAN ID	Identifiant numérique du VLAN à affecter aux points d'extrémité des membres du VLAN. La valeur doit être comprise entre 2 et 4 094. L'ID de VLAN 1 est réservé au VLAN par défaut et est utilisé pour les trames non balisées reçues par l'interface.
Description	Description qui identifie le VLAN.
Inter-VLAN Routing	Le routage Inter-VLAN est la capacité à acheminer le trafic entre les VLAN. Cochez la case **Disable** pour désactiver.

Port 1 **Port 2** **Port 3** **Port 4 (uniquement disponible sur le modèle RV134W)**	Vous pouvez associer les VLAN de l'appareil aux ports LAN du périphérique. Par défaut, tous les ports LAN appartiennent au VLAN1. Vous pouvez modifier ces ports pour les associer à d'autres VLAN. Choisissez le type de trame sortante pour chaque port : **Untagged** : l'interface est un membre non balisé du VLAN. Les trames du VLAN sont envoyées non balisées au port VLAN. **Tagged** : l'interface est un membre balisé du VLAN. Les trames du VLAN sont envoyées balisées au port VLAN. **Excluded** : le port n'est pas actuellement membre du VLAN. Il s'agit du paramètre par défaut de tous les ports à la création du VLAN.

ÉTAPE 4 Cliquez sur **Save**.

Pour modifier les paramètres d'un VLAN, sélectionnez le VLAN et cliquez sur **Edit**. Pour supprimer un VLAN sélectionné, cliquez sur **Delete**. Cliquez sur **Save** pour appliquer les modifications.

Configuration du DHCP statique

Vous pouvez configurer votre routeur afin qu'il affecte une adresse IP spécifique à un périphérique client doté d'une adresse MAC spécifique.

Pour configurer le DHCP statique :

ÉTAPE 1 Sélectionnez **Networking > LAN > Static DHCP**.

ÉTAPE 2 Dans le menu déroulant **VLAN**, sélectionnez un numéro de VLAN.

ÉTAPE 3 Cliquez sur **Add Row**.

ÉTAPE 4 Saisissez les informations suivantes :

Description	Description du client
IP Address	Adresse IP que vous souhaitez affecter au périphérique client. L'affectation DHCP statique signifie que le serveur DHCP affecte la même adresse IP à une adresse MAC définie chaque fois que le périphérique client est connecté au réseau. Le serveur DHCP affecte l'adresse IP réservée lorsque le périphérique client doté de l'adresse MAC correspondante demande une adresse IP.
MAC Address	Adresse MAC du périphérique client. Le format de l'adresse MAC est XX:XX:XX:XX:XX:XX, où X est un chiffre compris entre 0 et 9 (inclus) ou une lettre comprise entre A et F (inclus).

Pour modifier les paramètres d'un client DHCP statique, sélectionnez le client et cliquez sur **Edit**. Pour supprimer un client DHCP sélectionné, cliquez sur **Delete**. Cliquez sur **Save** pour appliquer les modifications.

Affichage des baux de clients DHCP

Vous pouvez afficher une liste de points d'extrémité sur le réseau (identifiés par nom d'hôte, adresse IP ou adresse MAC), et voir les adresses IP qui leur sont affectées par le serveur DHCP. Le VLAN des points d'extrémité est également affiché.

Pour voir les clients DHCP, sélectionnez **Networking > LAN > DHCP Leased Client Tables.**

Pour chaque VLAN défini sur l'appareil, une table présente une liste de clients associés au VLAN.

Pour affecter une adresse IP statique à l'un des appareils connectés :

ÉTAPE 1 Sur la ligne de l'appareil connecté, cochez la case **Add to Static DHCP**.

ÉTAPE 2 Cliquez sur **Save**.

Le serveur DHCP sur l'appareil affecte toujours l'adresse IP affichée lorsque le périphérique demande une adresse IP.

Configuration d'un hôte DMZ

Votre appareil prend en charge les zones démilitarisées ou DMZ. Une DMZ est un sous-réseau ouvert au public, bien que derrière le pare-feu. Une DMZ permet de rediriger des paquets qui arrivent sur l'adresse IP de votre port WAN vers une adresse IP particulière sur votre LAN.

Nous recommandons de placer les hôtes devant être exposés au WAN (comme les serveurs Web ou de messagerie) sur le réseau DMZ. Vous pouvez configurer des règles de pare-feu pour autoriser l'accès à des services et ports particuliers sur la DMZ, depuis le LAN ou depuis le WAN. En cas d'attaque d'un nœud de la DMZ, le réseau local n'est pas forcément vulnérable.

Vous devez configurer une adresse IP fixe (statique) pour le point d'extrémité qui doit servir d'hôte de la DMZ. Affectez à l'hôte de la DMZ une adresse IP sur le même sous-réseau que l'adresse IP LAN de l'appareil, mais distincte de l'adresse IP donnée à l'interface LAN de cette passerelle.

Pour configurer la DMZ :

ÉTAPE 1 Sélectionnez **Networking** > **LAN** > **DMZ Host**.

ÉTAPE 2 Cochez la case **Enable** pour activer la DMZ sur le réseau.

ÉTAPE 3 Dans le champ **Host IP Address**, saisissez l'adresse IP de l'hôte DMZ. L'hôte DMZ est le point d'extrémité qui reçoit les paquets redirigés.

ÉTAPE 4 Cliquez sur **Save**.

Gestion des ports

Vous pouvez configurer les paramètres de vitesse et de contrôle de flux des ports LAN du périphérique.

Pour configurer la vitesse des ports et le contrôle de flux :

ÉTAPE 1 Sélectionnez **Networking** > **Port Management**.

ÉTAPE 2 Précisez les informations suivantes :

Port	Numéro du port.
Link	Vitesse du port. Si aucun appareil n'est branché sur le port, ce champ affiche la mention **Down**.

Mode	Sélectionnez l'une des vitesses de port suivantes dans le menu déroulant : ▪ **Auto Negotiation** : l'appareil et le périphérique connecté sélectionnent une vitesse commune. ▪ **10Mbps Half** : 10 Mbit/s dans chaque direction, mais dans une seule direction à la fois. ▪ **10Mbps Full** : 10 Mbit/s dans chaque direction, simultanément. ▪ **100Mbps Half** : 100 Mbit/s dans chaque direction, mais dans une seule direction à la fois. ▪ **100Mbps Full** : 100 Mbit/s dans chaque direction, simultanément.
Flow Control	Cochez cette case pour activer le contrôle de flux sur le port. Le contrôle de flux consiste à gérer le débit des transmissions de données entre deux nœuds, afin d'empêcher un expéditeur trop rapide de submerger un récepteur trop lent. Il fournit un mécanisme qui permet au récepteur de contrôler la vitesse de transmission, afin que le nœud de réception ne soit pas submergé par les données provenant du nœud de transmission.
EEE	Cochez cette case pour activer le mode EEE (Energy-Efficient Ethernet) qui permet de réduire la consommation d'énergie durant les périodes de faible activité au niveau du transfert de données. Cette fonction est uniquement disponible sur le modèle RV134W.

ÉTAPE 3 Cliquez sur **Save**.

Configuration du routage

Utilisez la page Routing pour configurer le mode de fonctionnement et d'autres options de routage pour votre appareil.

Configuration du routage de base

Pour configurer le mode de routage de base :

ÉTAPE 1 Sélectionnez **Networking > Routing > Basic Routing**.

ÉTAPE 2 Dans la section **Static Routing section**, précisez les informations suivantes :

Route Entries	Sélectionnez le nombre d'entrées dans la liste déroulante.
Enter Route Name	Nom de l'acheminement.
Destination LAN IP	Adresse IP du réseau local de destination.
Subnet Mask	Adresse du masque de sous-réseau.
Gateway	Adresse de la passerelle.
Interface	Sélectionnez l'interface en cochant la case LAN & Wireless ou Internet (WAN).

ÉTAPE 3 Cliquez sur **Save**.

Configuration de Dynamic Routing Information Protocol (RIP)

Le protocole Routing Information Protocol est un protocole IGP (Interior Gateway Protocol) couramment utilisé sur les réseaux internes. Il permet au routeur d'échanger ses données de routage automatiquement avec d'autres routeurs, et d'ajuster dynamiquement ses tables de routage et de s'adapter aux changements sur le réseau.

Le routage dynamique RIP permet à l'appareil de s'adapter automatiquement aux modifications physiques de la topologie du réseau et d'échanger des tables de routage avec d'autres routeurs.

Le routeur détermine le chemin suivi par les paquets réseau, en visant le nombre le plus faible possible de sauts entre la source et la destination.

REMARQUE : Le protocole RIP est désactivé par défaut sur l'appareil.

Pour configurer le routage dynamique :

ÉTAPE 1 Sélectionnez **Networking** > **Routing** > RIP.

ÉTAPE 2 Dans la section RIP Basic Settings, configurez les paramètres suivants :

RIP Status	Cochez la case On pour activer ou la case Off pour désactiver l'option RIP.
RIP Version	Sélectionnez la version RIP (**RIPv1** ou **RIPv2** ou la valeur par défaut [réception de RIPv1, envoi de RIPv2]). La version de RIP utilisée pour envoyer des mises à jour de routage aux autres routeurs présents sur le réseau dépend de la configuration de ces autres routeurs. RIPv2 est compatible avec RIPv1.

ÉTAPE 3 Dans la zone RIP Members, cochez la case **Enable RIP** pour activer RIP sur toutes les interfaces disponibles (par ex., VLAN1, DSL_ATM, ETH_WAN, DSL_PTM).

ÉTAPE 4 Cliquez sur **Edit** pour spécifier les paramètres d'authentification RIP d'une interface :

ÉTAPE 5 Dans la section RIP Authentication Settings, dans Authentication, spécifiez la méthode d'authentification du port.

- **None :** choisissez cette option pour annuler l'authentification.
- **Simple Password Authentication** : choisissez cette option pour valider l'authentification par mot de passe simple. Saisissez le mot de passe dans le champ.
- **MD5 Authentication :** choisissez cette option pour valider l'authentification MD5.
- **MD5 Key ID** : saisissez un nombre compris entre 1 et 255. La valeur par défaut est 1.
- **MD5 Auth Key** : saisissez la clé d'authentification MD5 (longueur comprise entre 1 et 64 caractères).

ÉTAPE 6 L'interface passive détermine la façon dont le routeur reçoit les paquets RIP. Cochez la case **Passive Interface** pour activer sur le port.

ÉTAPE 7 Cliquez sur **Save**.

Affichage de la table de routage

La table de routage contient des informations sur la topologie du réseau dans l'environnement proche de celui-ci.

Pour afficher les informations de routage sur votre réseau, choisissez **Networking** > **Routing Table** et sélectionnez l'une des options suivantes :

- **Show IPv4 Routing Table** : la table de routage est affichée avec les champs configurés sur la page **Networking > Routing**.
- **Show IPv6 Routing Table** : la table de routage est affichée avec les champs configurés sur la page **Networking > IPv6**.

Configuration du DNS dynamique

Le DDNS (Dynamic DNS) est un service Internet qui permet de localiser les routeurs dotés d'adresses IP publiques variables à l'aide de noms de domaine Internet. Pour utiliser le DDNS, vous devez créer un compte auprès d'un fournisseur DDNS comme DynDNS.com ou noip.com.

Le routeur notifie des serveurs DNS dynamiques de modifications d'adresses IP WAN, afin que tout service public sur votre réseau puisse être contacté par le biais du nom de domaine.

Pour configurer le DDNS :

ÉTAPE 1 Sélectionnez **Networking** > **Dynamic DNS**.

ÉTAPE 2 Vous pouvez désactiver Dynamic DNS ou activer un **DDNS Service** sur l'appareil dans la liste déroulante.

ÉTAPE 3 Si vous sélectionnez l'option permettant d'activer l'un des services DDNS (DynDNS.com, noip.com), précisez les informations suivantes :

Username/E-mail Address	Nom d'utilisateur du compte DDNS ou adresse e-mail que vous avez utilisé pour créer le compte DDNS.
Password	Mot de passe du compte DDNS.
Verify Password	Permet de vérifier le mot de passe du DDNS.

Timeout	Définissez le délai (en heures) d'attente du périphérique.
Host Name	Nom du compte hôte.
Internet IP Address	(Lecture seule) Adresse IP Internet de votre appareil.
Status	(Lecture seule) Indique que la mise à jour DDNS s'est terminée correctement ou que l'envoi des informations de mise à jour du compte au serveur DDNS a échoué.

ÉTAPE 4 Cliquez sur **Test Configuration** pour tester la configuration DDNS.

ÉTAPE 5 Cliquez sur **Save**.

Configuration du mode IP

Les propriétés de réseau étendu peuvent être configurées pour les réseaux IPv4 et IPv6. Ces pages vous permettent de saisir des informations sur votre type de connexion Internet et d'autres paramètres.

Pour sélectionner un mode IP :

ÉTAPE 1 Sélectionnez **Networking** > **IP Mode**.

ÉTAPE 2 Dans le menu déroulant **IP Mode**, sélectionnez l'une des options suivantes :

LAN : IPv4, WAN : IPv4	Permet d'utiliser IPv4 sur les ports LAN et WAN.
LAN : IPv4+IPV6, WAN : IPv4+IPv6	Permet d'utiliser IPv4 et IPv6 sur les ports LAN et WAN.

ÉTAPE 3 Cliquez sur **Save**.

Configuration d'IPv6

Internet Protocol version 6 (IPv6) est une version du protocole Internet (IP) destinée à remplacer Internet Protocol version 4 (IPv4). La configuration des propriétés LAN d'un réseau IPv6 dépend du type de connexion Internet utilisé.

Configuration des connexions LAN IPv6

En mode IPv6, le serveur DHCP du réseau local (LAN) est activé par défaut (comme en mode IPv4). Le serveur DHCPv6 affecte des adresses IPv6 des groupes d'adresses qui utilisent la longueur de préfixe IPv6 affectée au LAN.

Pour configurer les paramètres LAN IPv6 sur votre appareil, vous devez d'abord définir le mode IP sur le mode suivant :

- LAN : IPv4+IPv6, WAN : IPv4+IPv6

Reportez-vous à la section **Configuration du mode IP** pour en savoir plus sur la définition du mode IP.

Pour configurer les paramètres de LAN IPv6 :

ÉTAPE 1 Sélectionnez **Networking** > **IPv6** > **IPv6 LAN Configuration**.

ÉTAPE 2 Saisissez les informations suivantes pour configurer l'adresse IPv6 du LAN :

IPv6 Address	Saisissez l'adresse IPv6 du périphérique. L'adresse IPv6 par défaut de la passerelle est fec0:1 (ou FEC0:0000:0000:0000:0000:0000:0000:0001). Vous pouvez modifier cette adresse IPv6 de 128 bits en fonction de la configuration de votre réseau.
IPv6 Prefix Length	Saisissez la longueur du préfixe IPv6. Le réseau (sous-réseau) IPv6 est identifié par les premiers bits de l'adresse, qui constituent le préfixe. Par défaut, le préfixe a une longueur de 64 bits. Tous les hôtes du réseau utilisent les mêmes premiers bits dans leur adresse IPv6. Vous réglez le nombre de bits initiaux communs des adresses du réseau dans ce champ.

ÉTAPE 3 Cliquez sur **Save** ou continuez pour configurer les paramètres LAN IPv6 DHCP.

ÉTAPE 4 Saisissez les informations suivantes pour configurer les paramètres du serveur (HCPv6) :

DHCP Status	Cochez cette option pour activer le serveur DHCPv6. Lorsque cette option est activée, l'appareil affecte une adresse IP incluse dans la plage spécifiée et fournit des informations supplémentaires à tout point d'extrémité du LAN qui demande des adresses DHCP.
Domain Name	(Facultatif) Nom de domaine du serveur DHCPv6.
Server Preference	Niveau de préférence serveur de ce serveur DHCP. Les messages d'annonce DHCP dotés de la valeur de préférence de serveur la plus élevée sont prioritaires sur les autres messages d'annonce DHCP. La valeur par défaut est 255.
DNS Server	Sélectionnez le nom du serveur DNS dans la liste déroulante.
Static DNS 1	Adresse IPv6 du serveur DNS principal du réseau IPv6 du FAI.
Static DNS 2	Adresse IPv6 du serveur DNS secondaire sur le réseau IPv6 du FAI.
Client Lease Time	Durée (en minutes) du bail du client pour des baux d'adresses IPv6 destinés aux points d'extrémité du LAN.

ÉTAPE 5 Dans la **Table IPv6 Address Pool**, cliquez sur **Add Row et saisissez les informations suivantes**.

Start Address	Adresse IPv6 de début du groupe.
End Address	Adresse IPv6 de fin du groupe.
IPv6 Prefix Length	Longueur de préfixe qui détermine le nombre de bits initiaux communs des adresses du réseau.

ÉTAPE 6 Cliquez sur **Save**.

Pour modifier les paramètres d'un groupe, sélectionnez le groupe et cliquez sur **Edit**. Pour supprimer un groupe sélectionné, cliquez sur **Delete**. Cliquez sur **Save** pour appliquer les modifications.

Configurer le routage IPv6 statique

Vous pouvez configurer des acheminements statiques pour diriger des paquets vers un réseau de destination. Un acheminement statique est un chemin prédéfini devant être emprunté par un paquet afin d'atteindre un hôte ou réseau particulier.

Certains FAI exigent un acheminement statique pour établir une table de routage au lieu d'utiliser des protocoles de routage dynamique. Les acheminements statiques ne requièrent pas de ressources de processeur pour l'échange des informations de routage avec un routeur homologue.

Vous pouvez également utiliser des acheminements statiques pour atteindre des routeurs homologues qui ne prennent pas en charge les protocoles de routage dynamique. Les acheminements statiques peuvent être utilisés avec des acheminements dynamiques. Prenez garde à ne pas introduire de boucles de routage dans votre réseau.

Pour créer un acheminement statique :

ÉTAPE 1 Sélectionnez **Networking** > **IPv6** > **IPv6 Static Routing**.

ÉTAPE 2 Dans la liste des acheminements statiques, cliquez sur **Add Row**.

ÉTAPE 3 Saisissez les informations suivantes :

Name	Nom de l'acheminement.
Destination	Adresse IPv6 de l'hôte ou réseau de destination pour cet acheminement.
Prefix Length	Nombre de bits de préfixe de l'adresse IPv6 qui définissent le sous-réseau de destination.
Gateway	Adresse IPv6 de la passerelle par laquelle l'hôte ou réseau de destination est joignable.
Interface	Interface pour l'acheminement : **LAN**, **WAN** ou **DSL-WAN**.

Metric	Priorité de l'acheminement. Sélectionnez une valeur comprise entre 2 et 15. S'il existe plusieurs acheminements vers une même destination, l'acheminement avec la métrique la plus faible est utilisé.
Active	Cochez cette option pour activer l'acheminement. Lorsque vous ajoutez un acheminement dans un état inactif, il apparaît dans la table de routage, mais n'est pas utilisé par l'appareil. La saisie d'un acheminement inactive peut être utile si l'acheminement n'est pas disponible au moment où vous l'ajoutez. Une fois le réseau disponible, vous pouvez activer l'acheminement.

ÉTAPE 4 Cliquez sur **Save**.

Pour modifier les paramètres d'un acheminement, sélectionnez-le et cliquez sur **Edit**. Pour supprimer un acheminement sélectionné, cliquez sur **Delete**. Cliquez sur **Save** pour appliquer les modifications.

Configuration du routage (RIPng)

RIP Next Generation (RIPng) est un protocole de routage basé sur l'algorithme D-V (Distance Vector). RIPng utilise des paquets UDP pour échanger des informations de routage par le port 521.

Le protocole RIPng utilise un nombre de sauts pour mesurer la distance jusqu'à la destination. Le nombre de sauts est appelé mesure, métrique ou coût. Le nombre de sauts d'un routeur vers un réseau auquel il est directement connecté est 0. Le nombre de sauts entre deux routeurs directement connectés est 1. Lorsque le nombre de sauts est supérieur ou égal à 16, le réseau ou l'hôte de destination est inaccessible.

Par défaut, l'actualisation du routage est envoyée toutes les 30 secondes. Si le routeur ne reçoit pas de mise à jour de l'acheminement d'un voisin après 180 secondes, les acheminements obtenus du voisin sont considérés comme injoignables. Si aucune mise à jour de l'acheminement n'est reçue après 240 secondes de plus, le routeur supprime ces acheminements de la table de routage.

Sur votre appareil, le protocole RIPng est désactivé par défaut.

Pour configurer RIPng :

ÉTAPE 1 Sélectionnez **Networking** > **IPv6** > **Routing (RIPng)**.

ÉTAPE 2 Dans le champ RIPng, cochez la case **Enable**.

ÉTAPE 3 Dans la table RIP Members, sélectionnez l'index et l'interface dans la liste et cochez la case **Enable** dans les colonnes RIPng et Passive Interface

ÉTAPE 4 Cliquez sur **Save**.

Configuration de l'annonce du routeur

Le démon RADVD (Router Advertisement Daemon) sur l'appareil est à l'écoute des messages de sollicitation du routeur sur le LAN IPv6 et répond par des annonces de routeur selon les besoins. Il s'agit d'une configuration IPv6 automatique sans état. L'appareil distribue les préfixes IPv6 à tous les nœuds du réseau.

Pour configurer le RADVD :

ÉTAPE 1 Sélectionnez **Networking** > **IPv6** > **Router Advertisement**.

ÉTAPE 2 Saisissez les informations suivantes :

RADVD Status	Cochez la case **Enable** pour activer le RADVD.
Advertise Mode	Sélectionnez l'un des modes suivants : **Unsolicited Multicast** : envoyez les annonces du routeur (RA) à toutes les interfaces appartenant au groupe de multidiffusion. **Unicast only** : limitez les annonces à des adresses IPv6 bien connues (les annonces du routeur ne sont envoyées qu'à l'interface appartenant à l'adresse connue).
Advertise Interval	Intervalle d'annonce (4 à 1 800) pour **Unsolicited Multicast**. La valeur par défaut est 30. L'intervalle d'annonce est une valeur aléatoire comprise entre les valeurs minimales et maximales d'intervalle d'annonce (MinRtrAdvInterval et MaxRtrAdvInterval). MinRtrAdvInterval = 0,33 * MaxRtrAdvInterval

RA Flags	Cochez la case **Managed** pour utiliser le protocole administré / avec état pour la configuration automatique des adresses. Cochez la case **Other** pour utiliser le protocole administré / avec état pour la configuration automatique d'autres informations (autres que l'adresse).
Router Preference	Sélectionnez **low**, **medium** ou **high** dans le menu déroulant. La valeur par défaut est medium. La préférence de routeur fournit une mesure de préférence pour les routeurs par défaut. Les valeurs low, medium et high sont signalées à l'aide de bits non utilisés dans les messages d'annonce du routeur. Cette extension est rétrocompatible, tant avec les routeurs (réglage de la valeur de préférence de routeur) qu'avec les hôtes (interprétation de la valeur de préférence de routeur). Ces valeurs sont ignorées par les hôtes qui ne mettent pas en œuvre la préférence de routeur. Cette fonction est utile lorsque d'autres appareils utilisant le RADVD sont présents sur le réseau local.
MTU	Taille de MTU (0 ou 1 280 à 1 500). La valeur par défaut est de 1 500 octets. Le MTU (Maximum Transmission Unit) correspond à la taille maximale de paquet pouvant être transmis sur le réseau. Le MTU est utilisé dans les annonces du routeur pour assurer que tous les nœuds du réseau utilisent la même valeur de MTU lorsque le MTU du réseau n'est pas connu.
Router Life Time	Valeur de durée de vie du routeur, ou durée en secondes d'existence des messages d'annonce sur le routeur. La valeur par défaut est 1 800 secondes.

ÉTAPE 3 Cliquez sur **Save**.

Configurer les préfixes d'annonces

Pour configurer les préfixes RADVD disponibles :

ÉTAPE 1 Sélectionnez **Networking** > **IPv6** > **Advertisement Prefixes**.

ÉTAPE 2 Cliquez sur **Add Row**.

ÉTAPE 3 Saisissez les informations suivantes :

IPv6 Prefix	Le préfixe IPv6 spécifie l'adresse réseau IPv6.
IPv6 Prefix Length	La variable de longueur de préfixe est une valeur décimale qui indique le nombre de bits contigus les plus significatifs de l'adresse qui composent la partie réseau de l'adresse.
Prefix Lifetime	Durée de vie du préfixe, ou durée durant laquelle le routeur à l'origine de la demande est autorisé à utiliser le préfixe.

ÉTAPE 4 Cliquez sur **Save**.

4

Réseaux sans fil

Sécurité sans fil

Les réseaux sans fil sont pratiques et simples à installer. Mais les réseaux sans fil fonctionnent en transmettant les informations par ondes radio, ce qui les rend potentiellement plus vulnérables que les réseaux traditionnels filaires.

Conseils relatifs à la sécurité des réseaux sans fil

Vous ne pouvez pas empêcher quelqu'un de se connecter à votre réseau sans fil, mais vous pouvez suivre les conseils suivants pour sécuriser votre réseau :

- Modifiez le nom ou SSID par défaut du réseau sans fil.

  Les appareils sans fil sont dotés d'un nom ou SSID de réseau sans fil par défaut. Il s'agit du nom de votre réseau sans fil, qui peut comporter jusqu'à 32 caractères.

  Pour protéger votre réseau, changez le nom de réseau sans fil par défaut et donnez-lui un nom unique qui le distingue des autres réseaux sans fil qui vous entourent.

  Lorsque vous choisissez un nom, n'utilisez pas d'informations personnelles, car elles seront accessibles à toute personne qui parcourt les réseaux sans fil.

- Modifiez le mot de passe par défaut.

  Sur les appareils sans fil comme les points d'accès, routeurs et passerelles, vous devez saisir un mot de passe lorsque vous souhaitez modifier les paramètres. Ces appareils ont un mot de passe par défaut. Le mot de passe par défaut est souvent cisco.

  Les pirates connaissent ces valeurs par défaut et essaient de les exploiter pour accéder à vos appareils sans fil et modifier vos paramètres réseau. Pour empêcher les accès non autorisés, personnalisez le mot de passe de l'appareil afin qu'il soit difficile à deviner.

- Activez le filtrage des adresses MAC.

  Les routeurs et passerelles Cisco vous permettent d'activer le filtrage d'adresses MAC. Vous pouvez autoriser les appareils spécifiés à accéder au réseau sans fil ou les en empêcher. L'adresse MAC est une série unique de chiffres et de lettres affectée à chaque appareil en réseau.

  Lorsque le filtrage des adresses MAC est activé, l'accès au réseau sans fil est réservé aux appareils sans fil dotés d'adresses MAC particulières. Vous pouvez par exemple spécifier l'adresse MAC de chaque ordinateur de votre réseau, afin que seuls ces ordinateurs puissent accéder à votre réseau sans fil.

- Activez le cryptage.

  Le cryptage protège les données transmises sur un réseau sans fil. Les normes WPA/WPA2 (Wi-Fi Protected Access) et WEP (Wired Equivalency Privacy) offrent différents niveaux de sécurité pour la communication sans fil. Actuellement, les appareils certifiés Wi-Fi sont tenus de prendre en charge la protection WPA2, mais ne sont pas obligés de prendre en charge l'authentification WEP.

  Un réseau crypté par WPA/WPA2 est mieux sécurisé qu'un réseau crypté en WEP, car le WPA/WPA2 utilise le cryptage par clé dynamique.

  Pour protéger les données qui transitent par les ondes, activez le niveau de cryptage le plus élevé pris en charge par vos équipements réseau.

  WEP est une norme de cryptage plus ancienne, mais certains appareils plus anciens n'offrent que cette option et ne prennent pas en charge le WPA.

- Utilisez des mots de passe complexes contenant au moins huit caractères. Combinez chiffres et lettres pour éviter l'utilisation de mots existants dans le dictionnaire.

Directives générales sur la sécurité réseau

Inutile de sécuriser le réseau sans fil si le réseau sous-jacent ne l'est pas. Nous vous recommandons de prendre les précautions suivantes :

- Protégez tous les ordinateurs sur le réseau et protégez individuellement les fichiers confidentiels par mot de passe.
- Changez les mots de passe à intervalles réguliers.
- Installez des logiciels antivirus et des logiciels de pare-feu individuels.
- Désactivez le partage de fichiers en point à point pour empêcher son utilisation par des applications sans votre accord.

Basic Wireless Settings

Réseaux sans fil sur votre appareil

Votre appareil fournit quatre réseaux sans fil virtuels ou quatre SSID (Service Set Identifier) : ciscosb1, ciscosb2, ciscosb3 et ciscosb4. Il s'agit des noms ou SSID par défaut de ces réseaux, mais vous pouvez les renommer à votre guise. Ces tableaux décrivent les paramètres par défaut de ces réseaux.

Nom SSID pour RV132W	ciscosb1	ciscosb2	ciscosb3	ciscosb4
Enabled	Oui	Non	Non	Non
SSID Broadcast	Activé	Activé	Activé	Activé
Security Mode	WPA2-Personal	Désactivé	Désactivé	Désactivé
MAC Filter	Désactivé	Désactivé	Désactivé	Désactivé
VLAN	1	1	1	1
Wireless Isolation with SSID	Désactivé	Désactivé	Désactivé	Désactivé
WMM	Activé	Activé	Activé	Activé
WPS	Activé	Désactivé	Désactivé	Désactivé

Nom SSID pour RV134W	ciscosb1_2.4G ou ciscosb1_5G	ciscosb2_2.4G ou ciscosb2_5G	ciscosb3_2.4G ou ciscosb3_5G	ciscosb4_2.4G ou ciscosb4_5G
Enabled	Oui	Non	Non	Non
SSID Broadcast	Activé	Désactivé	Désactivé	Désactivé
Security Mode	WPA2-Personal	Désactivé	Désactivé	Désactivé
MAC Filter	Désactivé	Désactivé	Désactivé	Désactivé

Nom SSID pour RV134W	ciscosb1_2.4G ou ciscosb1_5G	ciscosb2_2.4G ou ciscosb2_5G	ciscosb3_2.4G ou ciscosb3_5G	ciscosb4_2.4G ou ciscosb4_5G
VLAN	1	1	1	1
Wireless Isolation with SSID	Désactivé	Désactivé	Désactivé	Désactivé
WMM	Activé	Activé	Activé	Activé
WPS	Activé pour 2,4G mais désactivé par défaut pour 5G	Désactivé	Désactivé	Désactivé

Configuration des paramètres sans fil

Sélectionnez **Wireless > Basic Settings** pour configurer les paramètres sans fil de base.

Pour configurer les paramètres sans fil de base :

Sélectionnez **Wireless > Basic Settings**.

ÉTAPE 1 Dans le champ Radio, cochez la case **Enable** pour activer la radio sans fil. Par défaut, un seul réseau sans fil est activé (**ciscosb1**).

ÉTAPE 2 Dans le champ **Wireless Network Mode**, sélectionnez l'une des options suivantes dans la liste déroulante : (Pour l'option RV132W et RV134W 2,4G.)

B/G/N-Mixed	Si vous avez des appareils sans fil de type N, B et G sur votre réseau. Il s'agit du paramètre par défaut pour l'option RV132W et RV134 2,4G (recommandé).
B Only	Sélectionnez cette option si vous n'avez que des appareils sans fil de type B sur votre réseau.
G Only	Sélectionnez cette option si vous n'avez que des appareils sans fil de type G sur votre réseau.
N Only	Sélectionnez cette option si vous n'avez que des appareils sans fil de type N sur votre réseau.

B/G-Mixed	Sélectionnez cette option si vous n'avez que des appareils sans fil de type B et G sur votre réseau.
G/N-Mixed	Sélectionnez cette option si vous n'avez que des appareils sans fil de type G et N sur votre réseau.

ÉTAPE 3 Si vous sélectionnez le paramètre par défaut **B/G/N-Mixed,** la bande passante sans fil dans le champ Wireless Band Selection doit être définie à **20 MHz (option par défaut).** Si vous sélectionnez **N-Only** ou **G/N Mixed**, dans le champ Wireless Band Selection, sélectionnez la bande passante sans fil sur votre réseau **(20 MHz ou 20/40 MHz)**.

ÉTAPE 4 Facultatif et applicable pour configurer les paramètres de **largeur de bande sans fil RV134W 5G**.

A-Only	Sélectionnez cette option si vous n'avez que des appareils sans fil de type A sur votre réseau.
N/AC-Mixed	Sélectionnez cette option si vous n'avez que des appareils sans fil de type N et AC sur votre réseau.
A/N/AC-Mixed	Sélectionnez cette option si vous n'avez que des appareils sans fil de type A, N et AC sur votre réseau. Il s'agit du paramètre par défaut pour le RV134 5G (recommandé).

ÉTAPE 5 Dans le champ **Wireless Channel Width**, sélectionnez **80 MHZ** (valeur par défaut pour RV134W).

ÉTAPE 6 Dans le champ **U-APSD (WMM Power Save)**, cochez la case **Enable** pour activer la fonction U-APSD (Unscheduled Automatic Power Save Delivery), également appelée WMM Power Save, qui limite l'énergie consommée par les ondes radio.

U-APSD est un mécanisme d'économie d'énergie conçue pour les applications en temps réel, comme la VoIP, qui transfèrent les données en duplex intégral sur le réseau sans fil. En classifiant le trafic IP sortant en tant que données voix, les applications de ce type peuvent améliorer l'autonomie d'environ 25 % tout en limitant les délais de transmission.

ÉTAPE 7 (Facultatif) Dans la **table Wireless**, configurez les paramètres des quatre réseaux sans fil.

ÉTAPE 8 Cliquez sur **Save**.

Modification des paramètres de réseau sans fil

La Table Wireless de la page Basic Settings présente les paramètres des quatre réseaux sans fil pris en charge par l'appareil.

Pour configurer ces paramètres de réseau sans fil :

ÉTAPE 1 Cochez la case des réseaux que vous souhaitez configurer.

ÉTAPE 2 Cliquez sur **Edit.**

ÉTAPE 3 Configurez les paramètres suivants :

Enable SSID	Cliquez sur **On** pour activer le réseau.
SSID Name	Saisissez le nom du réseau.
SSID Broadcast	Cochez cette case pour activer la diffusion SSID. Si la diffusion SSID est activée, le routeur sans fil annonce sa disponibilité aux appareils sans fil dans la plage du routeur.
Security Mode	Reportez-vous à la section **Configuration du mode de sécurité**.
MAC Filter	Reportez-vous à la section **Configuration du filtrage MAC**.
VLAN	Sélectionnez le VLAN associé au réseau.
Wireless Isolation with SSID	Cochez cette case pour activer l'isolation sans fil au sein du SSID.
WMM (Wi-Fi Multimedia)	Cochez cette case pour activer le WMM.
WPS	Cochez cette case pour associer le bouton WPS du panneau avant à ce réseau.

ÉTAPE 4 Cliquez sur **Save**.

Configuration du mode de sécurité

Vous pouvez configurer l'un des modes de sécurité suivants pour les réseaux sans fil :

Configuring WEP

Le mode de sécurité WEP offre une sécurité faible en utilisant une méthode de cryptage simple et moins sûre que le WPA. La méthode WEP peut être nécessaire si vos appareils ne prennent pas en charge le WPA.

REMARQUE : Si vous n'êtes pas obligé d'utiliser le WEP, nous vous conseillons d'utiliser le WPA2. Si vous utilisez le mode sans fil N seulement, vous devez activer WPA2.

Pour configurer le mode de sécurité WEP :

ÉTAPE 1 Sélectionnez **Wireless > Basic Settings.** Dans la **table Wireless,** cochez la case correspondant au réseau que vous souhaitez configurer.

ÉTAPE 2 Cliquez sur **Edit Security Mode**. La page **Security Settings** apparaît.

ÉTAPE 3 Dans le champ **Select SSID**, sélectionnez le SSID dont vous souhaitez configurer les paramètres de sécurité.

ÉTAPE 4 Dans le menu **Security Mode**, sélectionnez **WEP**.

ÉTAPE 5 Dans le champ **Authentication Type**, sélectionnez l'une des options suivantes :

- **Open System** : il s'agit de l'option par défaut.
- **Shared Key** : sélectionnez cette option si votre administrateur réseau vous le demande. Dans le doute, sélectionnez l'option par défaut.

Dans les deux cas, les clients sans fil doivent fournir la bonne clé partagée (mot de passe) pour accéder au réseau sans fil.

ÉTAPE 6 Dans le champ **Encryption**, sélectionnez le type de cryptage :

- **10/64 bits (10 chiffres hexadécimaux)** : fournit une clé sur 40 bits.
- **26/128 bits (26 chiffres hexadécimaux)** : fournit une clé sur 104 bits dont le cryptage est plus difficile à décrypter. Nous recommandons le cryptage sur 128 bits.

ÉTAPE 7 (Facultatif) Dans le champ **Passphrase**, saisissez une expression alphanumérique (de plus de huit caractères pour une sécurité optimale) et cliquez sur **Generate Key** pour créer quatre clés WEP uniques dans les champs **WEP Key**.

Si vous préférez fournir votre propre clé, saisissez-la directement dans le champ **Key 1** (recommandé). La clé doit avoir une longueur de 5 caractères ASCII (ou 10 caractères hexadécimaux) pour le WEP 64 bits ou de 13 caractères ASCII (ou 26 caractères hexadécimaux) pour le WEP 128 bits. Les caractères hexadécimaux valables sont compris entre 0 et 9 et A et F.

ÉTAPE 8 Dans le champ **TX Key**, sélectionnez la clé que les appareils doivent utiliser comme clé partagée pour accéder au réseau sans fil.

ÉTAPE 9 Cliquez sur **Save** pour enregistrer vos paramètres.

ÉTAPE 10 Cliquez sur **Back** pour revenir à la page **Basic Settings**.

Configuration des modes WPA2-Personal et WPA2-Personal Mixed.

- Les modes de sécurité WPA2 Personal, WPA2 Personal Mixed, WPA2 Enterprise et WPA2 Enterprise Mixed fournissent une sécurité forte pour remplacer le WEP.
- **WPA2-Personal** : (Recommandé) WPA2 est la norme de sécurité spécifiée par le standard 802.11i finalisé. WPA2 prend en charge le cryptage AES et utilise une clé prépartagée (PSK) pour l'authentification.
- **WPA2-Personal Mixed** : permet aux clients WPA et WPA2 de se connecter simultanément en utilisant l'authentification PSK.

L'authentification personnelle correspond à la clé prépartagée qui est un mot de passe alphanumérique partagé avec le poste sans fil.

Pour configurer le mode de sécurité WPA2 Personal :

ÉTAPE 1 Dans la **table Wireless (Wireless > Basic Settings)**, cochez la case correspondant au réseau que vous souhaitez configurer.

ÉTAPE 2 Cliquez sur **Edit Security Mode.** La page **Security Settings** apparaît.

ÉTAPE 3 Dans le champ **Select SSID field**, sélectionnez le SSID dont vous souhaitez configurer les paramètres de sécurité.

ÉTAPE 4 Dans le menu **Security Mode**, sélectionnez l'une des deux options WPA2 Personal.

ÉTAPE 5 Dans le champ **Security Key**, saisissez une expression alphanumérique (8 à 63 caractères ASCII ou 64 chiffres hexadécimaux). L'échelle d'évaluation de la sécurité du mot de passe indique la robustesse de la clé : Inférieur au seuil minimum, faible, fort, très fort ou sécurisé. Nous vous recommandons d'utiliser une clé de sécurité considérée comme sécurisée sur l'échelle d'évaluation.

ÉTAPE 6 Pour afficher la clé de sécurité à mesure que vous la saisissez, cochez la case **Unmask Password**.

ÉTAPE 7 Dans le champ **Key Renewal**, saisissez l'intervalle de renouvellement de la clé (de 600 à 7 200 secondes). La valeur par défaut est 3 600.

ÉTAPE 8 Cliquez sur **Save** pour enregistrer vos paramètres. Cliquez sur **Back** pour revenir à la page **Basic Settings**.

Configuration des modes WPA2-Enterprise et WPA2-Enterprise Mixed

Les modes de sécurité WPA2 Enterprise et WPA2 Enterprise Mixed permettent d'utiliser l'authentification serveur RADIUS.

- **WPA2-Entreprise** : permet d'utiliser le WPA2 pour se connecter à l'aide de l'authentification par serveur RADIUS.
- **WPA2-Entreprise Mixed** : permet d'utiliser le client WPA2 pour se connecter à l'aide de l'authentification par serveur RADIUS.

Pour configurer le mode de sécurité WPA2 Enterprise :

ÉTAPE 1 Dans la **table Wireless (Wireless > Basic Settings)**, cochez la case correspondant au réseau que vous souhaitez configurer.

ÉTAPE 2 Cliquez sur **Edit Security Mode.**

ÉTAPE 3 Dans le champ **Select SSID**, sélectionnez le SSID dont vous souhaitez configurer les paramètres de sécurité.

ÉTAPE 4 Dans le menu **Security Mode**, sélectionnez l'une des deux options WPA2 Enterprise.

ÉTAPE 5 Dans le champ **RADIUS Server**, saisissez l'adresse IP du serveur RADIUS.

ÉTAPE 6 Dans le champ **RADIUS Port**, saisissez le port utilisé pour accéder au serveur RADIUS.

ÉTAPE 7 Dans le champ **Shared Key**, saisissez une expression alphanumérique.

ÉTAPE 8 Dans le champ **Key Renewal**, saisissez l'intervalle de renouvellement de la clé (de 600 à 7 200 secondes). La valeur par défaut est 3 600.

ÉTAPE 9 Cliquez sur **Save** pour enregistrer vos paramètres.

ÉTAPE 10 Cliquez sur **Back** pour revenir à la page **Basic Settings**.

Configuration du filtrage MAC

Vous pouvez utiliser le filtrage MAC pour accorder ou refuser l'accès au réseau sans fil en fonction de l'adresse MAC (matérielle) de l'appareil qui demande l'accès. Par exemple, vous pouvez saisir les adresses MAC d'un ensemble d'ordinateurs et n'autoriser l'accès au réseau qu'à ces ordinateurs. Vous pouvez configurer le filtrage MAC pour chaque réseau ou SSID.

Pour configurer le filtrage MAC :

ÉTAPE 1 Dans la **Table Wireless (Wireless > Basic Settings)**, cochez la case correspondant au réseau que vous souhaitez configurer.

ÉTAPE 2 Cliquez sur **Edit MAC Filtering.** La page **Wireless MAC Filter** apparaît.

ÉTAPE 3 Dans le champ **Edit MAC Filtering**, cochez la case **Enable** pour activer le filtrage MAC pour ce SSID.

ÉTAPE 4 Dans le champ **Connection Control**, sélectionnez le type d'accès au réseau sans fil :

- **Prevent** : sélectionnez cette option pour empêcher les appareils dont les adresses MAC sont incluses dans la **Table MAC Address** d'accéder au réseau sans fil. Cette option est sélectionnée par défaut.
- **Permit** : sélectionnez cette option pour autoriser les appareils dont les adresses MAC sont incluses dans la **Table MAC Address** à accéder au réseau sans fil.

ÉTAPE 5 Pour afficher les ordinateurs et autres appareils sur le réseau sans fil, cliquez sur **Show Client List**.

ÉTAPE 6 Dans le champ **Save to MAC Address Filter List**, cochez la case pour ajouter l'appareil à la liste des appareils à ajouter à la Table MAC Address.

ÉTAPE 7 Cliquez sur **Add to MAC** pour ajouter les appareils sélectionnés de la **Table Client List** à la **Table MAC Address.**

ÉTAPE 8 Cliquez sur **Save** pour enregistrer vos paramètres.

ÉTAPE 9 Cliquez sur **Back** pour revenir à la page **Basic Settings**.

Configurer l'accès par horaire

Pour renforcer la protection de votre réseau, vous pouvez restreindre l'accès en spécifiant les heures auxquelles les utilisateurs peuvent accéder au réseau.

Pour configurer l'accès par horaire :

ÉTAPE 1 Dans la **Table Wireless (Wireless > Basic Settings)**, cochez la case correspondant au réseau que vous souhaitez configurer.

ÉTAPE 2 Cliquez sur **Time of Day Access**. La page Time of Day Access apparaît.

ÉTAPE 3 Dans le champ **Active Time**, cochez la case **Enable** pour activer Time of Day Access.

ÉTAPE 4 Dans les champs **Start Time** et **Stop Time**, spécifiez la plage horaire durant laquelle l'accès au réseau sera autorisé.

ÉTAPE 5 Cliquez sur **Save**.

Configuration des paramètres sans fil avancés

Les paramètres sans fil avancés sont réservés à un administrateur expert, car un mauvais réglage peut diminuer les performances sans fil.

Pour configurer les paramètres sans fil avancés :

ÉTAPE 1 Sélectionnez **Wireless > Advanced Settings.** La page Advanced Settings apparaît.

ÉTAPE 2 Configurez les paramètres suivants :

Frame Burst	Activez cette option pour accélérer les performances de vos réseaux sans fil, en fonction du fabricant de vos appareils réseau. Si vous n'êtes pas sûr de la manière d'exploiter cette option, conservez l'état par défaut (activé).
WMM No Acknowledgment	L'activation de l'option WMM No Acknowledgment peut entraîner une amélioration du débit, mais aussi du taux d'erreurs dans un environnement radio (RF) saturé. Par défaut, ce paramètre est désactivé.

Basic Rate	Le paramètre Basic Rate ne correspond pas à la vitesse de transmission, mais à une série de débits de transmission de la plateforme Services Ready Platform. L'appareil annonce sa vitesse de base aux autres appareils sans fil de votre réseau, afin qu'ils connaissent les débits qui seront utilisés. La plate-forme prête pour les services annonce également qu'elle sélectionnera automatiquement la meilleure vitesse de transmission. Le paramètre par défaut est Default, lorsque l'appareil peut transmettre à tous les débits sans fil standard (1 Mbit/s, 2 Mbits/s, 5,5 Mbits/s, 11 Mbits/s, 18 Mbits/s, 24 Mbits/s, 36 Mbits/s, 48 Mbits/s et 54 Mbits/s). L'appareil prend en charge les débits N en plus des débits B et G. Les autres options sont 1-2 Mbits/s, pour une utilisation avec une technologie sans fil plus ancienne, et All, lorsque l'appareil peut transmettre à toutes les vitesses sans fil. La vitesse de base ne correspond pas à la vitesse réelle de transmission des données. Pour spécifier la vitesse de transmission des données de l'appareil, configurez le paramètre Transmission Rate.
Transmission Rate	Vous devez régler la vitesse de transmission en fonction de la vitesse de votre réseau sans fil. Vous pouvez effectuer votre sélection parmi une plage de vitesses de transmission ou vous pouvez sélectionner **Auto** pour que l'appareil utilise automatiquement le débit de données le plus rapide et pour activer la fonction de négociation automatique. La fonction de négociation automatique négocie la meilleure vitesse de connexion possible entre l'appareil et un client sans fil. La valeur par défaut est Auto.
N Transmission Rate	Vous devez régler la vitesse de transmission en fonction de la vitesse de votre réseau sans fil de type N. Vous pouvez effectuer votre sélection parmi une plage de vitesses de transmission ou vous pouvez sélectionner **Auto** pour que l'appareil utilise automatiquement le débit de données le plus rapide et pour activer la fonction de négociation automatique. La fonction de négociation automatique négocie la meilleure vitesse de connexion possible entre l'appareil et un client sans fil. La valeur par défaut est Auto.

CTS Protection Mode	L'appareil utilise automatiquement le mode de protection CTS (Clear-To-Send) si vos appareils sans fil de type N et G rencontrent des problèmes et ne parviennent pas à transmettre vers l'appareil lorsque le trafic 802.11b environnant est très important. Cette fonction renforce la capacité de l'appareil à capter les transmissions sans fil de type N et G, au prix d'une diminution importante des performances. La valeur par défaut est Auto.
Beacon Interval	La valeur d'intervalle de balise indique la fréquence d'émission de la balise. Une balise est un paquet diffusé par l'appareil pour synchroniser le réseau sans fil. Saisissez une valeur comprise entre 40 et 3 500 millisecondes. La valeur par défaut est 100.
DTIM Interval	Cette valeur comprise entre 1 et 255 correspond à l'intervalle du message DTIM (Delivery Traffic Indication Message). Un champ DTIM est un champ de compte à rebours qui informe les clients de la prochaine fenêtre d'écoute des messages de diffusion et de multidiffusion. Lorsque les messages de diffusion ou de multidiffusion pour les clients associés sont stockés dans la mémoire tampon de l'appareil, celui-ci envoie le message DTIM suivant avec une valeur d'intervalle DTIM. Les clients entendent les balises et sortent de veille pour recevoir les messages de diffusion ou de multidiffusion. La valeur par défaut est 1.
Fragmentation Threshold	Cette valeur indique la taille maximale d'un paquet au-delà de laquelle les données sont scindées en plusieurs paquets. Si vous rencontrez une quantité importante d'erreurs de paquets, essayez d'augmenter légèrement le seuil de fragmentation. Un réglage trop faible du seuil de fragmentation peut dégrader les performances du réseau. Seule une légère réduction de la valeur par défaut est recommandée. Dans la majorité des cas, conservez la valeur par défaut de 2 346.

RTS Threshold	En cas de flux de données intermittent, essayez une réduction mineure. La valeur par défaut de 2 347 est recommandée. Lorsque la taille d'un paquet réseau est inférieure au seuil RTS (Request to Send) prédéfini, le mécanisme RTS/CTS (Clear to Send) n'est pas enclenché. La plate-forme prête pour les services envoie des trames RTS à une station de réception et négocie l'envoi d'une trame de données. Après réception d'un RTS, la station sans fil répond par une trame CTS pour autoriser le début de la transmission.

ÉTAPE 3 Cliquez sur **Save**.

Configuration de WPS

Configurez le WPS (Wi-Fi Protected Setup) pour permettre aux appareils compatibles WPS de se connecter aisément et en toute sécurité au réseau sans fil. Reportez-vous à la documentation de votre appareil client pour en savoir plus sur sa configuration WPS.

Pour configurer WPS :

ÉTAPE 1 Sélectionnez **Wireless > WPS**. La page Wi-Fi Protected Setup s'affiche.

ÉTAPE 2 Cliquez sur **Edit** pour changer le réseau sans fil sur lequel vous souhaitez activer WPS.

ÉTAPE 3 Configurez le WPS sur les appareils clients de l'une des trois manières suivantes :

- Cliquez ou appuyez sur le bouton **WPS** de l'appareil client, puis cliquez sur l'icône WPS de cette page.
- Saisissez le code **PIN WPS** du client, puis cliquez sur Register.
- Un appareil client nécessite un code PIN de ce routeur ; utilisez le code PIN du routeur indiqué.

  Device PIN : identifie le code PIN d'un appareil essayant de se connecter.

PIN Lifetime : durée de vie de la clé. À l'expiration de cette période, une nouvelle clé est négociée.

Enable AP with Enrollee PIN : cochez cette case pour rendre l'option « PIN Lifetime » modifiable manuellement.

Preshared Key : choisissez « Add Client to existing network (Use Existing PSK) » ou « Reconfigure network (Generate New PSK) ».

Une fois que vous avez configuré le WPS, les informations suivantes sont affichées en haut de la page WPS : Wi-Fi Protected Setup Status, Network Name (SSID) et Security.

5

Pare-feu

Vous pouvez sécuriser votre réseau en créant et en appliquant des règles utilisées par le routeur pour bloquer et autoriser le trafic Internet entrant et sortant de façon sélective. Vous pouvez ensuite spécifier les appareils concernés par ces règles et la façon dont elles s'appliquent. Pour ce faire, vous devez définir les éléments suivants :

- Les types de services ou de trafic que le routeur doit autoriser ou bloquer. Par exemple, la navigation Web, la VoIP, ou d'autres services standard et personnalisés que vous définissez.
- La direction du trafic en spécifiant la source et la destination dans les champs From Zone (LAN/WAN/DMZ) et To Zone (LAN/WAN/DMZ).
- Les horaires d'application des règles par le routeur.
- Les mots-clés (d'un nom de domaine ou d'une adresse URL d'une page Web) que le routeur doit autoriser ou bloquer.
- Règles autorisant ou bloquant le trafic Internet entrant et sortant pour certains services à certaines heures
- Adresses MAC des appareils dont les accès entrants doivent être bloqués par le routeur
- Les déclencheurs de ports qui indiquent au routeur d'autoriser ou de bloquer l'accès à certains services définis par leur numéro de port.
- Les rapports et les alertes que vous souhaitez recevoir du routeur

Vous pouvez par exemple définir des règles d'accès restreint en fonction d'un horaire, d'une adresse Web ou de mots-clés d'adresses Web. Vous pouvez bloquer l'accès Internet d'applications et de services sur le réseau local (LAN), comme les forums de discussion ou les jeux. Vous pouvez bloquer l'accès par le réseau étendu (WAN) ou la DMZ publique à des groupes d'ordinateurs spécifiques sur votre réseau.

Les règles entrantes (WAN vers LAN/DMZ) limitent l'accès du trafic entrant sur votre réseau, n'autorisant l'accès à certaines ressources locales qu'à certains utilisateurs externes. Par défaut, tous les accès au réseau LAN non sécurisé provenant du réseau WAN non sécurisé sont bloqués, à l'exception des réponses aux requêtes provenant du LAN ou de la DMZ. Pour autoriser des appareils externes à accéder à des services sur le LAN sécurisé, vous devez définir une règle de pare-feu pour chaque service.

Si vous souhaitez autoriser le trafic entrant, l'adresse IP du port WAN du routeur doit être rendue publique. Cela s'appelle « exposer votre hôte ». La manière de rendre votre adresse publique dépend de la configuration des ports WAN pour l'appareil. Vous pouvez utiliser l'adresse IP si une adresse statique est affectée au port WAN, ou un nom DDNS (Dynamic DNS) si l'adresse de votre WAN est dynamique.

Les règles sortantes (LAN/DMZ vers WAN) limitent l'accès du trafic sortant de votre réseau, n'autorisant l'accès à certaines ressources externes qu'à certains utilisateurs locaux. La règle sortante par défaut est d'autoriser l'accès depuis la zone sécurisée (LAN) à la DMZ publique ou au WAN non sécurisé. Pour bloquer l'accès à Internet (WAN non sécurisé) par des hôtes du LAN sécurisé, vous devez créer une règle de pare-feu pour chaque service.

Paramètres de base du pare-feu

Pour configurer les paramètres de base du pare-feu :

ÉTAPE 1 Sélectionnez **Firewall > Basic Settings**.

ÉTAPE 2 Configurez les paramètres de pare-feu suivants :

SPI Firewall	Cochez la case **Enable** pour activer le pare-feu.
DoS Protection	Cochez la case **Enable** pour activer la protection contre les attaques de déni de service (DoS ou Denial of Service).
Block Ping WAN Interface	Cochez la case **Enable** pour bloquer l'interface WAN Ping.
SSH Access	Cochez la case **Enable** pour activer l'accès SSH.
Remote SSH Access	Cochez la case **Enable** pour activer l'accès SSH à distance.

Web Access	Sélectionnez le type d'accès Web autorisé pour la connexion au pare-feu : HTTP, Redirect HTTP traffic to HTTPS ou HTTPS (secure HTTP).
Remote Web Access	Cochez la case **Enable** pour activer l'accès Web à distance et sélectionnez la connexion : HTTP ou HTTPS.
Remote Upgrade	Pour autoriser la mise à niveau à distance du routeur, cochez la case **Enable**.
Allowed Remote IP Address	Cliquez sur le bouton **Any IP Address** pour autoriser la gestion à distance à partir de toute adresse IP ou spécifiez une adresse IP spécifique dans le champ d'adresse.
Remote Management Port	Saisissez le port sur lequel l'accès à distance est autorisé. Le port par défaut est 443. Lorsque vous accédez au routeur à distance, vous devez saisir le port de gestion à distance dans le cadre de l'adresse IP. Par exemple : **https://<remote-ip>:<port_à_distance> ou https://168.10.1.11:443**
IPv4 Multicast Passthrough (IGMP Proxy)	Cochez la case **Enable** pour activer l'intercommunication de multidiffusion pour IPv4.
IPv6 Multicast Passthrough (IGMP Proxy)	Cochez la case **Enable** pour activer l'intercommunication de multidiffusion pour IPv6.
Unicast RPF	Unicast Reverse Path Forwarding (Unicast RPF) peut contribuer à limiter le trafic malicieux sur un réseau d'entreprise. Il agit en vérifiant l'accessibilité de l'adresse source dans les paquets transmis. Il peut limiter l'apparence des adresses usurpées sur un réseau. Si l'adresse IP source n'est pas valide, le ticket est rejeté. Dans les routeurs RV132W/RV134W, Unicast RPF fonctionne en mode strict ou en mode lâche. En mode strict, le paquet doit être reçu sur l'interface que le routeur utilise pour transmettre le paquet de retour. En mode lâche, l'adresse source doit apparaître dans la table de routage. Dans Unicast RPF, sélectionnez l'une des options suivantes dans la liste déroulante (**Disable unicast, Strict unicast** ou **Loose unicast**).

SIP ALG	Cochez la case **Enable** pour autoriser le trafic de protocole d'initiation de session (SIP) à traverser le pare-feu.
UPnP	Cochez la case **Enable** pour activer le protocole UPnP.
Allow Users to Configure	Cochez la case **Enable** pour autoriser la définition de règles de correspondances de ports UPnP par les utilisateurs utilisant des ordinateurs ou d'autres appareils compatibles UPnP. Si la case est décochée, l'appareil n'autorise pas l'application à ajouter la règle de redirection.
Allow Users to Disable Internet Access	Cochez la case **Enable** pour autoriser les utilisateurs à désactiver l'accès à Internet.
Block Java	Cochez cette case pour bloquer les applets Java. Les applets Java sont de petits programmes intégrés dans les pages Web qui activent des fonctions dynamiques de la page. Un applet malveillant peut servir à compromettre ou infecter un ordinateur. Activez ce paramètre pour bloquer le téléchargement des applets Java. Cliquez sur **Auto** pour bloquer Java automatiquement ou sur **Manual** pour spécifier un port sur lequel Java doit être bloqué.
Block Cookies	Cochez cette case pour bloquer les cookies. Les sites Web utilisent les cookies pour stocker les informations relatives à l'ouverture des sessions. Toutefois, certains sites Web utilisent les cookies pour surveiller l'utilisateur et ses habitudes de navigation. Activez cette option pour empêcher la création de cookies par les sites Web. De nombreux sites Web ne sont pas accessibles lorsque les cookies sont refusés. Le blocage des cookies peut donc entraîner un dysfonctionnement de ces sites. Cliquez sur **Auto** pour bloquer automatiquement les cookies ou sur **Manual** pour spécifier un port sur lequel les cookies doivent être bloqués.

Block ActiveX	Cochez cette case pour bloquer le contenu ActiveX. Les contrôles ActiveX, similaires aux applets Java, sont installés sur les ordinateurs Windows qui utilisent Internet Explorer. Les contrôles ActiveX malveillants peuvent servir à compromettre ou infecter un ordinateur. Activez ce paramètre pour bloquer le téléchargement des contrôles ActiveX. Cliquez sur **Auto** pour bloquer ActiveX automatiquement ou sur **Manual** pour spécifier un port sur lequel ActiveX doit être bloqué.
Block Proxy	Cochez cette case pour bloquer les serveurs proxy. Un serveur mandataire ou proxy permet à un ordinateur d'acheminer les connexions aux autres ordinateurs par le biais du proxy, contournant ainsi certaines règles de pare-feu. Par exemple, lorsque les connexions à une adresse IP spécifique sont bloquées par une règle de pare-feu, ces requêtes peuvent être acheminées par le biais d'un proxy qui n'est pas bloqué par la règle, contournant ainsi la règle concernée. Activez cette option pour bloquer les serveurs proxy. Cliquez sur **Auto** pour bloquer automatiquement les serveurs proxy ou sur **Manual** pour spécifier un port sur lequel les serveurs proxy doivent être bloqués.

ÉTAPE 3 Cliquez sur **Save**.

AVERTISSEMENT Lorsque la connexion Web à distance est activée, le routeur est accessible par tout utilisateur qui connaît l'adresse IP correspondante. Un utilisateur extérieur malveillant pouvant reconfigurer l'appareil, il est vivement conseillé de modifier le mot de passe administrateur et le mot de passe invité avant de continuer.

Configuration de la gestion des horaires

Vous pouvez créer des horaires afin d'appliquer les règles de pare-feu certains jours ou à certaines heures de la journée.

Ajout ou modification d'un horaire de pare-feu

Pour créer ou modifier un horaire :

ÉTAPE 1 Sélectionnez **Firewall** > **Schedule Management**.

ÉTAPE 2 Cliquez sur **Add Row**.

ÉTAPE 3 Dans le champ **Name**, saisissez un nom unique pour identifier l'horaire. Le nom est disponible dans la liste **Select Schedule** sur la page Firewall Rule Configuration page (Reportez-vous à la section **Configuration des règles d'accès**).

ÉTAPE 4 Dans la section **Scheduled Days**, indiquez si vous souhaitez appliquer l'horaire à tous les jours ou à certains jours. Si vous sélectionnez **Specific Days**, cochez les cases en regard des jours que vous souhaitez inclure dans l'horaire.

ÉTAPE 5 Dans la section **Scheduled Time of Day**, sélectionnez le moment où vous souhaitez appliquer l'horaire. Si vous choisissez **Specific Time**, saisissez l'heure de début et l'heure de fin.

ÉTAPE 6 Cliquez sur **Save**.

Configuration de la gestion des services

Lorsque vous créez une règle de pare-feu, vous pouvez spécifier un service contrôlé par la règle. Différents types de services courants sont disponibles et vous pouvez créer vos propres services.

La page **Services Management** permet de créer des services personnalisés auxquels les règles de pare-feu sont appliquées. Une fois défini, le nouveau service apparaît dans la table **Available Custom Services**.

Pour créer un service personnalisé :

ÉTAPE 1 Sélectionnez **Firewall** > **Service Management**.

ÉTAPE 2 Cliquez sur **Add Row**.

ÉTAPE 3 Dans le champ **Service Name**, saisissez le nom du service à des fins d'identification et de gestion.

ÉTAPE 4 Dans le champ **Protocol**, sélectionnez le protocole Layer 4 utilisé par le service dans la liste déroulante :

- **TCP**
- **UDP**
- **TCP et UDP**
- **ICMP**
- **ICMPv6**
- **Autre**

ÉTAPE 5 Dans le champ **Start Port**, saisissez le premier port TCP ou UDP de la plage utilisée par le service.

ÉTAPE 6 Dans le champ **End Port**, saisissez le dernier port TCP ou UDP de la plage utilisée par le service.

ÉTAPE 7 Si vous sélectionnez le champ ICMP Type, saisissez le type de protocole ICMP.

ÉTAPE 8 Si vous sélectionnez un autre protocole, saisissez son numéro.

ÉTAPE 9 Cliquez sur **Save**.

Pour modifier une entrée, sélectionnez-la et cliquez sur **Edit**. Apportez les modifications souhaitées, puis cliquez sur **Save**.

Configuration des règles d'accès

Configuration de la stratégie appliquée par défaut au trafic sortant

La page **Access Rules** permet de configurer la stratégie sortante par défaut pour le trafic acheminé du réseau sécurisé (LAN) vers le réseau non sécurisé (WAN dédié/facultatif).

La stratégie entrante par défaut pour le trafic provenant de la zone non sécurisée en direction de la zone sécurisée est toujours bloquée et ne peut pas être modifiée.

REMARQUE : Les stratégies d'accès à Internet remplacent les règles d'accès lorsqu'elles sont toutes deux configurées sur l'appareil.

Pour configurer la stratégie sortante par défaut :

ÉTAPE 1 Sélectionnez **Firewall** > **Access Rules**.

ÉTAPE 2 Sélectionnez **Allow** ou **Deny**.

REMARQUE : Vérifiez que la prise en charge d'IPv6 est activée sur le routeur pour configurer un pare-feu IPv6.

ÉTAPE 3 Cliquez sur **Save**.

Réorganisation des règles d'accès

L'ordre dans lequel les règles d'accès sont affichées dans la table des règles d'accès indique l'ordre dans lequel elles sont appliquées. Vous pouvez réorganiser la table pour que certaines règles s'appliquent avant d'autres. Par exemple, si vous voulez appliquer une règle qui autorise certains types de trafic avant de bloquer d'autres types de trafic.

Pour réorganiser les règles d'accès :

ÉTAPE 1 Sélectionnez **Firewall > Access Rules**.

ÉTAPE 2 Cliquez sur **Reorder**.

ÉTAPE 3 Cochez la case dans la ligne de la règle que vous souhaitez déplacer vers le haut ou le bas et cliquez sur la flèche vers le haut ou le bas pour déplacer la règle d'une ligne vers le haut ou vers le bas, ou sélectionnez la position voulue de la règle dans la liste déroulante et cliquez sur **Move to**.

ÉTAPE 4 Cliquez sur **Save**.

Ajout de règles d'accès

Toutes les règles de pare-feu configurées sur le routeur sont affichées dans la **Table Access Rules**. Cette liste indique également si la règle est activée et présente un récapitulatif de la zone source/cible, ainsi que les services et les utilisateurs concernés par la règle.

Pour créer une règle d'accès :

ÉTAPE 1 Sélectionnez **Firewall > Access Rules**.

ÉTAPE 2 Cliquez sur **Add Row**.

ÉTAPE 3 Dans le champ **Connection Type**, sélectionnez la direction du trafic :

- **Outbound (LAN > WAN)** : sélectionnez cette option pour créer une règle sortante.
- **Inbound (WAN > LAN)** : sélectionnez cette option pour créer une règle entrante.
- **Inbound (WAN > DMZ)** : sélectionnez cette option pour créer une règle entrante.
- **Inter-VLAN (VLAN > VLAN)** : sélectionnez cette option pour créer une règle inter VLA.
- **Inter-VLAN (VLAN > DMZ)** : sélectionnez cette option pour créer une règle inter VLA.

ÉTAPE 4 Dans la liste déroulante **Action**, sélectionnez l'action :

- **Always Block** : toujours bloquer le type de trafic sélectionné.
- **Always Allow** : ne jamais bloquer le type de trafic sélectionné.
- **Block by schedule** : bloque le type de trafic sélectionné en fonction d'un horaire.
- **Allow by schedule** : autorise le type de trafic sélectionné en fonction d'un horaire.

ÉTAPE 5 Dans la liste déroulante **Services**, sélectionnez le service à autoriser ou bloquer pour cette règle. Sélectionnez **All Traffic** pour appliquer la règle à tous les services et applications, ou sélectionnez une application particulière à bloquer :

- DNS (Domain Name System), UDP ou TCP
- File Transfer Protocol (FTP)
- Hypertext Transfer Protocol (HTTP)
- Secure Hypertext Transfer Protocol (HTTPS)
- Trivia File Transfer Protocol (TFTP)
- Internet Message Access Protocol (IMAP)
- Network News Transport Protocol (NNTP)
- Post Office Protocol (POP3)
- Simple Network Management Protocol (SNMP)

- Simple Mail Transfer Protocol (SMTP)
- Telnet
- STRMWORKS
- Terminal Access Controller Access-Control System (TACACS)
- Telnet (commande)
- Telnet secondaire
- Telnet SSL
- Voice (SIP)

ÉTAPE 6 Dans le champ **Source ID**, sélectionnez les utilisateurs auxquels appliquer la règle :

- **Any** : la règle s'applique au trafic provenant de tout hôte du réseau local.
- **Single Address** : la règle s'applique au trafic provenant d'une adresse IP spécifique du réseau local. Saisissez l'adresse dans le champ **Start**.
- **Address Range** : la règle s'applique au trafic provenant d'une adresse IP appartenant à une plage d'adresses spécifique. Saisissez l'adresse IP de début dans le champ **Start** et l'adresse IP de fin dans le champ **Finish**.

ÉTAPE 7 Dans la liste déroulante **Source IP**, sélectionnez les adresses IP source à partir desquelles la règle bloque ou autorise les paquets.

- **Any** : la règle s'applique à toutes les adresses IP source.
- **Single Address** : saisissez une adresse IP unique à laquelle la règle s'applique dans le champ Start.
- **Address Range** : saisissez une plage d'adresses IP à laquelle la règle s'applique dans les champs Start et Finish.

ÉTAPE 8 Dans la liste déroulante **Destination IP**, sélectionnez les adresses IP de destination vers lesquelles la règle bloque ou autorise les paquets.

- **Any** : la règle s'applique à toutes les adresses IP de destination.
- **Single Address** : saisissez une adresse IP unique à laquelle la règle s'applique dans le champ Start.
- **Address Range** : saisissez une plage d'adresses IP à laquelle la règle s'applique dans les champs Start et Finish.

ÉTAPE 9 Pour consigner les détails de tous les paquets correspondant à la règle, sélectionnez **Always** dans la liste déroulante. Exemple : si une règle sortante pour un horaire est réglée sur **Block Always**, chaque fois qu'un paquet tente d'établir une connexion sortante pour le service concerné, un message contenant l'adresse source et de destination du paquet (ainsi que d'autres informations) est enregistré dans le journal.

L'activation de la journalisation peut engendrer un volume conséquent de messages de journal et n'est recommandée qu'à des fins de débogage.

Sélectionnez **Never** pour désactiver la journalisation.

REMARQUE : lorsque le trafic va du LAN ou de la DMZ vers le WAN, le système exige la réécriture de l'adresse IP source ou de destination des paquets IP entrants lorsqu'ils transitent par le pare-feu.

ÉTAPE 10 **Rule Status :** cochez la case **Enable** pour activer la nouvelle règle d'accès.

ÉTAPE 11 Cliquez sur **Save**.

Configuration de la stratégie d'accès à Internet

Le routeur prend en charge plusieurs options permettant de bloquer l'accès à Internet. Vous pouvez bloquer l'ensemble du trafic Internet, le bloquer au niveau de certains ordinateurs ou points d'extrémité ou encore bloquer l'accès à des sites Internet en spécifiant des mots-clés spécifiques. Si ces mots-clés sont détectés dans le nom d'un site (URL du site, nom d'un newsgroup, etc.), le site est bloqué.

Ajout ou modification d'une stratégie d'accès à Internet

Pour créer une règle d'accès à Internet, procédez comme suit :

ÉTAPE 1 Sélectionnez **Firewall** > **Internet Access Policy**.

ÉTAPE 2 Cliquez sur **Add Row**.

ÉTAPE 3 Cochez **Status Enable**.

ÉTAPE 4 Saisissez un nom de stratégie à des fins d'identification et de gestion.

ÉTAPE 5 Dans la liste déroulante **Action**, sélectionnez le type de restriction d'accès souhaité :

- **Always block** : toujours bloquer le trafic Internet. Cette option bloque le trafic Internet en provenance et en direction de tous les points d'extrémité. Si vous souhaitez bloquer l'intégralité du trafic, mais autoriser certains points d'extrémité à recevoir du trafic Internet, reportez-vous à l'étape 7.

- **Always allow** : toujours autoriser le trafic Internet. Vous pouvez affiner ce paramètre afin de bloquer certains points d'extrémité spécifiés du trafic Internet. Pour cela, reportez-vous à l'étape 7. Vous pouvez également autoriser l'ensemble du trafic Internet à l'exception de certains sites Web ; reportez-vous à l'étape 8.
- **Block by schedule** : bloque le trafic Internet selon un horaire précis (par exemple, si vous souhaitez bloquer le trafic Internet pendant les heures de travail, mais l'autoriser après les heures de travail et pendant le week-end).
- **Allow by schedule** : autorise le trafic Internet en fonction d'un horaire.

Si vous sélectionnez **Block by schedule** ou **Allow by schedule**, cliquez sur **Configure Schedules** pour créer un horaire. Reportez-vous à la section **Configuration de la gestion des horaires**.

ÉTAPE 6 Sélectionnez un horaire dans la liste déroulante.

ÉTAPE 7 (Facultatif) Appliquez la stratégie d'accès à des ordinateurs particuliers afin d'autoriser ou de bloquer le trafic provenant d'appareils particuliers :

a. Dans la table **Apply Access Policy to the Following PCs**, cliquez sur **Add Row**.

b. Dans la liste déroulante **Type**, sélectionnez le mode d'identification de l'ordinateur (adresse MAC, adresse IP ou plage d'adresses IP).

c. En fonction du choix effectué à l'étape précédente, saisissez l'une des valeurs suivantes dans le champ **Value** :

- L'adresse MAC (xx:xx:xx:xx:xx:xx) de l'ordinateur ciblé par la politique.
- L'adresse IP de l'ordinateur ciblé par la stratégie.
- Les adresses IP de début et de fin de la plage d'adresses à bloquer (comme 192.168.1.2-192.168.1.253).

ÉTAPE 8 Pour bloquer le trafic de sites Web particuliers :

a. Dans la table **Website Domain Name & Keyword**, cliquez sur **Add Row**.

b. Dans la liste déroulante **Type**, sélectionnez le mode de blocage d'un site Web (en spécifiant le nom de domaine ou un mot-clé qui est inclus dans l'URL).

c. Dans le champ **Value**, saisissez le **Nom de domaine, l'URL** ou le **Mot-clé** utilisé pour bloquer le site Web.

Par exemple, pour bloquer l'URL exemple.com, sélectionnez **URL Address** dans la liste déroulante, puis saisissez **exemple.com** dans le champ **Value**. Pour bloquer une URL contenant le mot-clé « exemple », sélectionnez **Keyword** dans la liste déroulante et saisissez **exemple** dans le champ **Value**.

ÉTAPE 9 Cliquez sur **Save**.

Configuration NAT un-à-un

Utilisez la page One-to-one Network Translation (NAT) pour mapper des adresses IP locales derrière votre pare-feu à des adresses IP globales. Le NAT un-à-un est un mécanisme permettant à des systèmes configurés avec des adresses IP privées et situés derrière un pare-feu d'apparaître comme disposant d'adresses IP publiques.

Pour ajouter une règle de NAT un-à-un :

ÉTAPE 1 Sélectionnez **Firewall > One-to-One NAT**.

ÉTAPE 2 Cliquez sur **Add Row**.

ÉTAPE 3 Dans le champ **Private Range Begin**, saisissez la première adresse IP de la plage d'adresses IP (LAN) privées.

ÉTAPE 4 Dans le champ **Public Range Begin**, saisissez la première adresse IP de la plage d'adresses IP (WAN) publiques.

ÉTAPE 5 Dans **Range Length**, saisissez le nombre d'adresses IP publiques qui doivent être mappées aux adresses privées.

ÉTAPE 6 Dans le champ **Service**, sélectionnez le service auquel la règle s'applique. Les services de NAT un à un vous permettent de configurer le service que l'adresse IP privée (LAN) doit accepter lorsque du trafic est envoyé à l'adresse IP publique correspondante. Les services configurés sur les adresses IP de la plage sont acceptés lorsque du trafic est disponible sur l'adresse IP publique correspondante.

ÉTAPE 7 Cliquez sur **Save.**

Configuration de la redirection de port individuel.

La redirection de ports sert à rediriger le trafic Internet d'un port du réseau WAN vers un autre port du réseau LAN. Des services courants sont disponibles, mais vous pouvez également définir un service personnalisé et les ports associés pour la redirection. Pour ajouter une règle de redirection de port individuel :

ÉTAPE 1 Sélectionnez **Firewall** > **Single Port Forwarding**. Une liste préexistante d'applications s'affiche.

ÉTAPE 2 Dans le champ **Application**, saisissez le nom de l'application pour laquelle vous souhaitez configurer la redirection de port.

ÉTAPE 3 Dans le champ **External Port**, saisissez le numéro de port qui déclenche la règle en cas de demande de connexion émise par le trafic sortant.

ÉTAPE 4 Dans le champ **Internal Port**, saisissez le numéro de port utilisé par le système distant pour répondre à la demande qu'il reçoit.

ÉTAPE 5 Dans la liste déroulante **Protocol**, sélectionnez un protocole (**TCP, UDP** ou **TCP** et **UDP**).

ÉTAPE 6 Dans la liste déroulante **Interface**, sélectionnez **DSL_ATM_WAN, DSL_PTM_WAN, ETH_WAN ou USB_WAN**.

ÉTAPE 7 Dans le champ **IP Address**, saisissez l'adresse IP de l'hôte, côté LAN, vers laquelle le trafic IP spécifique doit être redirigé. Par exemple, vous pouvez rediriger le trafic HTTP vers le port 80 de l'adresse IP d'un serveur Web côté LAN.

ÉTAPE 8 Dans le champ **Enable**, cochez la case **Enable** pour activer la règle.

ÉTAPE 9 Cliquez sur **Save**.

Configuration de la redirection de plages de ports

Pour ajouter une règle de redirection de plage de ports :

ÉTAPE 1 Sélectionnez **Firewall** > **Port Range Forwarding**.

ÉTAPE 2 Dans le champ **Application**, saisissez le nom de l'application pour laquelle vous souhaitez configurer la redirection de port.

ÉTAPE 3 Dans le champ **Start**, spécifiez le numéro de port de début de la plage de ports à rediriger.

ÉTAPE 4 Dans le champ **End**, spécifiez le numéro de port de fin de la plage de ports à rediriger.

ÉTAPE 5 Dans la liste déroulante **Protocol**, sélectionnez un protocole (**TCP**, **UDP** ou **TCP** et **UDP**).

ÉTAPE 6 Dans la liste déroulante **Interface**, sélectionnez **DSL_ATM_WAN, DSL_PTM_WAN, ETH_WAN ou USB_WAN**.

ÉTAPE 7 Dans le champ **IP Address**, saisissez l'adresse IP de l'hôte, côté LAN, vers laquelle le trafic IP spécifique doit être redirigé.

ÉTAPE 8 Dans le champ **Enable**, cochez la case **Enable** pour activer la règle.

ÉTAPE 9 Cliquez sur **Save**.

Configuration du déclenchement de plage de ports

Le déclenchement de plages de ports permet aux appareils du LAN ou de la DMZ de demander qu'un ou plusieurs ports soient redirigés vers eux. Le mécanisme de déclenchement de port attend une demande sortante du LAN/DMZ sur l'un des ports sortants définis, puis ouvre un port entrant pour le type de trafic concerné.

Le déclenchement des ports est une forme de redirection de ports dynamiques lorsqu'une application transmet des données sur les ports entrants et sortants ouverts. Il ouvre un port entrant pour un type de trafic particulier sur un port sortant défini. Cette option est plus souple que la redirection de port statique (disponible lors de la configuration de règles de pare-feu), car il n'est pas nécessaire que la règle cible une adresse IP ni une plage IP du réseau LAN. En outre, les ports sont fermés lorsqu'ils ne sont pas utilisés, offrant ainsi un niveau de sécurité supérieur à la redirection de ports.

REMARQUE : La redirection de port ne s'applique pas aux serveurs du LAN, en raison de la dépendance sur l'appareil LAN qui établit une connexion sortante avant l'ouverture des ports entrants.

Pour fonctionner correctement, certaines applications doivent recevoir des données sur un port particulier ou une plage de ports particulière lorsque des appareils externes s'y connectent. Le routeur doit envoyer toutes les données entrantes pour cette application uniquement au port ou à la plage de ports spécifiques. La passerelle dispose d'une liste d'applications et de jeux avec des ports entrants et sortants associés à ouvrir. Vous pouvez également spécifier une règle de déclenchement de ports en spécifiant le type de trafic (TCP ou UDP) et la plage de ports entrants et sortants à ouvrir.

Pour ajouter une règle de déclenchement de port :

ÉTAPE 1 Sélectionnez **Firewall** > **Port Range Triggering**.

ÉTAPE 2 Dans le champ **Application**, saisissez le nom de l'application pour laquelle vous souhaitez configurer la redirection de port.

ÉTAPE 3 Dans le champ **Triggered Range**, saisissez le numéro de port ou la plage de numéros de ports qui déclenche la règle en cas de demande de connexion émise par le trafic sortant. Si la connexion sortante n'utilise qu'un seul port, saisissez le même numéro de port dans les deux champs.

ÉTAPE 4 Dans les champs **Forwarded Range**, saisissez le numéro de port ou les numéros de plage de ports utilisés par le système distant pour répondre à la demande qu'il reçoit. Si la connexion entrante n'utilise qu'un seul port, saisissez le même numéro de port dans les deux champs.

ÉTAPE 5 Dans la liste déroulante **Interface**, sélectionnez **DSL_ATM, DSL_PTM, ETH_WAN,** ou **USB_WAN.**

ÉTAPE 6 Dans le champ **Enable**, cochez la case **Enable** pour activer la règle.

ÉTAPE 7 Cliquez sur **Save**.

Configuration de la protection contre les attaques

Utilisez la page **Attack Protection** pour déterminer le mode de protection de votre réseau contre certains types d'attaques classiques, notamment la détection, l'inondation et l'intrusion Echo Storm.

ÉTAPE 1 Cliquez sur **Firewall > Attack Protection**.

ÉTAPE 2 Vérifiez ce qui suit et saisissez une plage numérique pour chacun :

- **SYN Flood Detect Rate :** saisissez le nombre maximal de paquets SYN par seconde qui amène le dispositif de sécurité à déterminer qu'une intrusion par inondation SYN se produit. Saisissez une valeur comprise entre 0 et 10 000 paquets SYN par seconde. La valeur par défaut est de 128 paquets SYN par seconde. Une valeur nulle (0) indique que la fonction de détection d'inondation SYN est désactivée.

- **Echo Storm :** saisissez le nombre de commandes ping qui amènent le dispositif de sécurité à déterminer qu'un événement d'intrusion Echo Storm se produit. Saisissez une valeur comprise entre 0 et 10 000 paquets ping par seconde. La valeur par défaut est de 100 paquets ping par seconde. Une valeur nulle (0) indique que la fonction Echo Storm est désactivée.
- **ICMP Flood :** saisissez le nombre de paquets ICMP par seconde, notamment de paquets PING, qui amènent le dispositif de sécurité à déterminer qu'un événement d'intrusion par inondation ICMP se produit. Saisissez une valeur comprise entre 0 et 10 000 paquets ICMP par seconde. La valeur par défaut est de 100 paquets ICMP par seconde. Une valeur nulle (0) indique que la fonction d'inondation ICMP est désactivée.
- **Block UDP Flood :** cochez cette case pour empêcher le dispositif de sécurité d'accepter plus de 150 connexions UDP actives simultanées par seconde à partir d'un seul ordinateur sur le réseau LAN et saisissez une valeur comprise entre 0 et 10 000 (valeur par défaut = 1 000).
- **Block TCP Flood :** cochez cette case pour abandonner tous les paquets TCP non valides et saisissez une valeur comprise entre 0 et 10 000 (valeur par défaut = 200). Cette fonction protège votre réseau d'une attaque par inondation SYN, dans laquelle un pirate envoie une succession de requêtes (de synchronisation) SYN à un système cible.

ÉTAPE 3 Cliquez sur **Save**.

Configuration des paramètres de session

Vous pouvez déterminer le nombre maximal de sessions non identifiées et semi-ouvertes sur les routeurs Cisco RV132W/RV134W. Vous pouvez également créer des délais d'expiration des sessions TCP et UDP pour vous assurer que le trafic Internet sur votre réseau privé répond à vos attentes.

Pour configurer les paramètres de session :

ÉTAPE 1 Sélectionnez **Firewall > Session Setting.**

ÉTAPE 2 Dans le champ **TCP Session Timeout**, saisissez le délai, en secondes, au bout duquel les sessions TCP inactives sont supprimées de la table des sessions. La plupart des sessions TCP prennent normalement fin lorsque les indicateurs RST ou FIN sont détectés. Cette valeur doit être comprise entre 18 000 et 432 000 secondes. La valeur par défaut est de 86 400 secondes (24 heures).

ÉTAPE 3 Dans le champ **UDP Timeout**, saisissez le délai, en secondes, au bout duquel les sessions UDP inactives sont supprimées de la table des sessions. Cette valeur doit être comprise entre 90 et 360 secondes. La valeur par défaut est de 180 secondes (3 minutes).

ÉTAPE 4 Dans le champ **ICMP Timeout**, saisissez le délai, en secondes, au bout duquel les sessions ICMP inactives sont supprimées de la table des sessions. Cette valeur doit être comprise entre 15 et 60 secondes. La valeur par défaut est de 30 secondes.

6

VPN

VPN site-à-site

Les VPN site-à-site sont mis en œuvre sur la base des stratégies IPsec qui sont affectées aux topologies VPN. Une stratégie IPsec est un ensemble de paramètres qui définissent les caractéristiques du VPN site-à-site, tels que les protocoles et algorithmes de sécurité qui seront utilisés pour sécuriser le trafic dans un tunnel IPsec.

Configuration VPN de base

Votre appareil prend en charge le VPN IPsec site-à-site pour un tunnel VPN passerelle-à-passerelle unique. Une fois ces paramètres VPN de base configurés, vous pouvez vous connecter en toute sécurité à un autre routeur VPN. Par exemple, vous pouvez configurer votre appareil sur le site d'une filiale pour qu'il se connecte à un routeur, qui lui-même se connecte aux tunnels VPN site-à-site présents sur le site de l'entreprise, ceci afin que le site de la filiale puisse accéder en toute sécurité au réseau de l'entreprise.

Pour configurer les paramètres VPN de base d'une connexion IPsec site-à-site :

ÉTAPE 1 Sélectionnez **VPN > Site-to-Site IPsec VPN > Basic VPN Setup**.

ÉTAPE 2 Dans le champ **New Connection Name**, attribuez un nom au tunnel VPN.

ÉTAPE 3 Dans le champ **Pre-Shared Key**, saisissez la clé prépartagée, ou le mot de passe, qui sera échangée entre les deux routeurs. La clé prépartagée doit comporter entre 8 et 49 caractères.

ÉTAPE 4 Dans le champ **Protocol**, sélectionnez le nom du protocole dans le menu déroulant

ÉTAPE 5 Dans les champs **Endpoint Information**, saisissez les informations suivantes :

- **Remote Endpoint** : indiquez si le routeur auquel votre appareil se connecte est identifié par son adresse IP ou par un nom de domaine complet. Par exemple, une adresse IP telle que 192.168.1.1 ou un nom de domaine complet tel que cisco.com.

- **Remote WAN (Internet) IP Address** : saisissez l'adresse IP publique ou le nom de domaine du point d'extrémité distant.
- **Local WAN (Internet) IP Address** : est généré automatiquement.
- Dans les champs **Secure Connection Remote Accessibility**, saisissez les informations suivantes :
- **Remote LAN (Local Network) IP Address** : adresse de réseau privé (LAN) du point d'extrémité distant. Il s'agit de l'adresse IP du réseau interne pour le site distant.
- **Remote LAN Subnet Mask** : masque de sous-réseau du réseau privé (LAN) du point d'extrémité distant.
- **Local LAN (Local Network) IP Address** : adresse de réseau privé (LAN) du réseau local. Il s'agit de l'adresse IP du réseau interne sur l'appareil.
- **Local LAN (Local Network) Subnet Mask** : masque de sous-réseau du réseau privé (LAN) du réseau local.

REMARQUE : Les adresses IP de WAN distant et de LAN distant ne peuvent pas exister sur le même sous-réseau. Par exemple, l'adresse IP de LAN distant 192.168.1.100 et l'adresse IP de LAN local 192.168.1.115 créent un conflit lorsque le trafic est acheminé via le VPN. Le troisième octet doit être différent pour que les adresses IP soient sur des sous-réseaux différents. Par exemple, l'adresse IP de LAN distant 192.168.1.100 et l'adresse IP de LAN local 192.168.2.100 sont acceptées.

ÉTAPE 6 Cliquez sur **Save.**

Affichage des valeurs par défaut

Cliquez sur **View Default Settings** pour afficher les valeurs par défaut utilisées dans les paramètres VPN de base. Ces valeurs sont proposées par le VPN Consortium (VPNC) et supposent que vous utilisez une clé prépartagée ou un mot de passe connu de votre appareil et du point d'extrémité distant.

Configuration des paramètres VPN avancés

Les paramètres VPN avancés tels que les stratégies IKE et d'autres stratégies VPN déterminent la façon dont l'appareil initie et reçoit des connexions VPN.

Pour configurer les paramètres VPN avancés, sélectionnez VPN > Site-to-Site IPsec VPN > Advanced VPN Setup.

Traversée NAT

La technique de traversée NAT (Network Address Translation, traduction d'adresses réseau) est une méthodologie de mise en réseau informatique visant à établir et à maintenir des connexions au protocole Internet sur des passerelles qui mettent en œuvre la traduction d'adresses réseau (**NAT**).

ÉTAPE 1 Pour activer la traversée NAT, dans le champ **NAT Traversal**, cochez la case **Enable.**

Gestion des stratégies IKE

Le protocole IKE (Internet Key Exchange) échange des clés entre deux passerelles IPsec de manière dynamique. Vous pouvez créer des stratégies IKE afin de définir les paramètres de sécurité à utiliser pour l'échange de données avec le routeur distant via la connexion VPN IPsec. Par exemple, vous pouvez créer des stratégies IKE afin de définir des paramètres pour l'authentification de l'homologue et les algorithmes de cryptage. Assurez-vous que les paramètres de cryptage, d'authentification et de clé-groupe de votre stratégie VPN sont compatibles avec les paramètres définis sur le routeur distant.

Pour ajouter une stratégie IKE :

ÉTAPE 1 Sur la page **Advanced VPN Setup**, dans la table IKE Policy, cliquez sur **Add Row**.

ÉTAPE 2 Dans le champ **Policy Name**, attribuez un nom unique à la stratégie IKE.

ÉTAPE 3 Dans le champ **Mode Exchange**, choisissez l'un des modes suivants pour la stratégie :

- **Main** : négocie le tunnel avec une sécurité supérieure, mais est plus lent.
- **Agressive** : établit plus rapidement la connexion, mais la sécurité est moindre.

ÉTAPE 4 Dans les champs **Local Identifier** et **Remote Identifier**, indiquez si vous souhaitez identifier votre appareil et le routeur distant à l'aide d'une des options suivantes :

- Local WAN IP : adresse IP du réseau WAN
- IP Address : adresse IP définie par l'utilisateur sous forme d'ID
- FQDN : utilisez un nom de domaine complet sous forme d'ID
- USER FQDN : adresse électronique ou autre ID.
- DER ASN1 DN : nom distinctif du certificat. Lorsque vous choisissez cette option, saisissez le nom de sujet du certificat de l'appareil. Le format de la chaîne est « C=US/ST=sjc/L=cisco/0=cisco/OU=smb/CN=RV134W ».

ÉTAPE 5 Dans la section **IKE SA Parameters**, configurez les paramètres pour définir la robustesse et le mode de négociation de l'association de sécurité (Security Association, SA) entre votre appareil et le routeur distant :

a. Dans le champ **Encryption Algorithm**, sélectionnez l'algorithme utilisé pour crypter les données.

b. Dans le champ **Authentication Algorithm**, spécifiez l'algorithme d'authentification de l'en-tête VPN : Vérifiez que l'algorithme d'authentification est configuré de manière identique sur les deux extrémités du tunnel VPN.

- Dans le champ **Authentication Method**, sélectionnez l'une des options suivantes :
- **Pre-Shared Key** : les homologues VPN utilisent une clé prépartagée pour s'authentifier mutuellement.
- **Certificate** : les homologues VPN utilisent un certificat pour s'authentifier mutuellement. Lorsque la méthode d'authentification est Certificate :
  - L'identifiant local/distant peut être défini sur « DER ASN1 DN » avec la valeur du nom distinctif du certificat.
  - L'identifiant local/distant peut également être défini sur Local WAN IP, FQDN, USER FQDN, dès lors que le SubjectAltName du certificat possède les mêmes type/valeur que l'identifiant. Cela signifie également que si la demande CSR du certificat est générée par l'appareil (dans le menu VPN > Site-to-Site IPSec VPN > Certificate Management > Generate CSR), les paramètres « IP Address », « Domain Name » ou « Email Address » doivent être renseignés avec la valeur appropriée.

c. Dans le champ **Diffie-Hellman (DH) Group**, spécifiez l'algorithme de groupe DH qui est utilisé lors de l'échange d'une clé prépartagée. Le groupe DH définit la robustesse de l'algorithme, en bits. Vérifiez que le groupe DH est configuré de manière identique des deux côtés de la stratégie IKE.

d. Dans le champ **SA-Lifetime**, saisissez l'intervalle, en secondes, au bout duquel l'association de sécurité n'est plus valide.

e. Pour activer la fonction **Dead Peer Detection**, cochez la case **Enable**. La détection d'homologue indisponible (Dead Peer Detection, DPD) permet de détecter si l'homologue est actif. Si l'homologue est identifié comme étant indisponible, l'appareil supprime l'association de sécurité IPsec et IKE. Si vous activez cette fonction, saisissez également les paramètres suivants :

- **DPD Delay** : intervalle, en secondes, entre les messages DPD R-U-THERE consécutifs. Les messages DPD R-U-THERE sont envoyés à chaque intervalle.

- **Failure Count** : ce champ indique le nombre d'échecs. La valeur par défaut est 3. L'appareil considère que l'homologue est inactif s'il ne reçoit pas la réponse DPP de l'homologue pour ce nombre de fois.
- **DPD Action** : sélectionnez l'option Terminate pour mettre fin à la session ou l'option Reconnect pour vous reconnecter.

f. **Extended Authentication** : permet d'activer XAUTH.

ÉTAPE 6 Cliquez sur **Save.**

REMARQUE : (Pour le modèle RV132W uniquement) Si une connexion VPN est déjà configurée, vous devez la supprimer pour ajouter une autre connexion VPN.

Gestion des stratégies VPN

REMARQUE : Avant de créer une stratégie VPN automatique, veillez à créer la stratégie IKE à partir de laquelle vous souhaitez créer la stratégie VPN automatique.

Pour gérer les stratégies VPN :

ÉTAPE 1 Sélectionnez **VPN > Site-to-Site IPsec VPN > Advanced VPN Setup**. Dans la table VPN Policy, cliquez sur **Add Row**.

ÉTAPE 2 Dans la section **Add / Edit VPN Policy Configuration** :

a. Dans le champ **Policy Name**, saisissez un nom unique permettant d'identifier la stratégie.

b. Dans le champ **Policy Type**, choisissez l'une des options suivantes :

- **Auto Policy** : certains paramètres du tunnel VPN sont générés automatiquement. Cette option nécessite l'utilisation du protocole IKE (Internet Key Exchange) pour les négociations entre les deux points d'extrémité VPN.
- **Manual Policy** : tous les paramètres (y compris les clés) du tunnel VPN sont saisis manuellement pour chaque point d'extrémité. Aucun serveur tiers ni aucune organisation tierce n'est impliqué(e).

c. **VPN Failover** : cochez la case **Enable** pour activer le basculement VPN. Si cette option est activée, la configuration de l'interface est grisée. Le tunnel VPN exploite toujours l'interface WAN active.

d. **Interface** : sélectionnez l'interface WAN sur laquelle le tunnel VPN est défini.

e. **Redundant Enable** : lorsque cette option est sélectionnée, si l'appareil ne parvient pas à établir le tunnel avec le « point d'extrémité distant » (configuré sur la même page), il tente d'établir le tunnel avec le « point d'extrémité distant redondant ».

f. **Redundant Remote Endpoint :** sélectionnez le type d'identifiant de passerelle à fournir sur le point d'extrémité distant : **IP Address** ou **FQDN**. Saisissez l'adresse IP ou le nom de domaine complet.

g. **Redundant Remote Identifier Type** : sélectionnez le type d'identifiant distant redondant dans la liste déroulante : **Local Wan IP, IP Address, FQDN, User-FDQN** ou **DER ASN1 DN.**

ÉTAPE 3 **NetBIOS** : les ordinateurs exécutant Microsoft Windows® communiquent entre eux via des paquets de diffusion NetBIOS. Pour permettre à NetBIOS d'accéder aux ressources du réseau distant, parcourez le voisinage réseau Windows®.

ÉTAPE 4 Dans les sections **Local Traffic Selection** et **Remote Traffic Selection** :

- Dans les champs **Local IP et Remote IP**, indiquez le nombre d'extrémités à inclure dans la stratégie VPN :
  - **Single** : limite la stratégie à un seul hôte. Saisissez l'adresse IP de l'hôte qui fera partie du VPN dans le champ **IP Address**.
  - **Subnet** : permet à un ensemble de sous-réseau de se connecter au VPN. Saisissez l'adresse réseau dans le champ **IP Address**, puis le masque de sous-réseau dans le champ **Subnet Mask**. Saisissez l'adresse IP réseau du sous-réseau dans le champ **IP Address**. Saisissez le masque de sous-réseau, tel que 255.255.255.0, dans le champ **Subnet Mask**. Le champ affiche automatiquement l'adresse de sous-réseau par défaut qui est basée sur l'adresse IP.

REMARQUE : N'utilisez pas de sous-réseaux qui se chevauchent pour les sélecteurs de trafic local et distant. L'utilisation de ces sous-réseaux nécessite l'ajout de routes statiques sur le routeur et les hôtes à utiliser. Par exemple, évitez :

Sélecteur de trafic local : 192.168.1.0/24

Sélecteur de trafic distant : 192.168.0.0/16

ÉTAPE 5 **Split DNS** : permet au routeur de trouver le serveur DNS du routeur distant sans passer par le FAI (Internet). Si vous activez la fonction Split DNS, saisissez également les paramètres suivants : Domain Name Server 1-2, Domain 1-6. Le nom de domaine Server1-2 résoudra le nom de domaine 1-6.

ÉTAPE 6 **Manual Policy Parameters** : pour un type de stratégie **Manual**, saisissez les paramètres dans la section **Manual Policy Parameters** :

- **Protocol** : sélectionnez le protocole dans la liste déroulante : **ESP** ou **AH.**

- **SPI-Incoming, SPI-Outgoing** : saisissez une valeur hexadécimale composée de 3 à 8 caractères (0x1234, par exemple). L'index des paramètres de sécurité (Security Parameter Index, SPI) identifie l'association de sécurité des flux de trafic entrant et sortant.
- **Encryption Algorithm** : sélectionnez l'algorithme utilisé pour crypter les données.
- **Key-In, Key-Out** : saisissez la clé de cryptage de la stratégie appliquée au trafic entrant et sortant. La longueur de la clé dépend de l'algorithme de cryptage choisi :
  - 3DES : 24 caractères
  - AES-128 : 16 caractères
  - AES-192 : 24 caractères
  - AES-256 : 32 caractères
- **Integrity Algorithm** : sélectionnez l'algorithme utilisé pour vérifier l'intégrité des données.
- **Key-In, Key Out** : saisissez la clé d'intégrité (pour l'ESP avec mode d'intégrité) de la stratégie appliquée au trafic entrant et sortant. La longueur de la clé dépend de l'algorithme choisi :
  - MD5 : 16 caractères
  - SHA-1 : 20 caractères
  - SHA2-256 : 32 caractères
  - Aucun, SHA2-384, SHA2-512

ÉTAPE 7 Pour le type de stratégie **Auto**, saisissez les paramètres dans la section **Auto Policy Parameters**. **SA-Lifetime** : saisissez la durée de l'association de sécurité en secondes. À la fin de l'intervalle indiqué en secondes, l'association de sécurité est renégociée. La valeur par défaut est 3 600 secondes. La valeur minimale est 30 secondes.

- **Protocol** : sélectionnez le protocole dans la liste déroulante : **ESP** ou **AH.**
- **Encryption Algorithm** : sélectionnez l'algorithme utilisé pour crypter les données.
- **Integrity Algorithm** : sélectionnez l'algorithme utilisé pour vérifier l'intégrité des données.

- **PFS Key Group :** cochez la case **Enable** pour activer PFS (Perfect Forward Secrecy) afin de renforcer la sécurité. Ce protocole est plus lent, mais contribue à empêcher l'écoute électronique en garantissant qu'un échange Diffie-Hellman a lieu pour chaque négociation de phase 2.
- **DH Group :** spécifiez l'algorithme de groupe DH utilisé lors de l'échange d'une clé prépartagée. Le groupe DH définit la robustesse de l'algorithme, en bits. Vérifiez que le groupe DH est configuré de manière identique des deux côtés de la stratégie IKE.
- **Select IKE Policy** : sélectionnez la stratégie IKE qui définira les caractéristiques de la négociation des associations de sécurité.

ÉTAPE 8 Cliquez sur **Save**.

Configuration du concentrateur et du spoke

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

CONSEIL Il sera peut-être utile de créer une fiche technique répertoriant l'adresse IP LAN, le sous-réseau LAN et le masque de sous-réseau pour chaque site. Lors de la configuration sur un site spoke, vous nécessitez les adresses réseau du site principal et de tous les autres sites spoke. Lors de la configuration sur un site concentrateur, vous nécessitez les adresses réseau de tous les sites spoke.

Concentrateur	Spoke1	Spoke2
192.168.1.100	192.168.75.100	192.168.74.100
192.168.1.0	192.168.75.0	192.168.74.0
255.255.255.0	255.255.255.0	255.255.255.0

Configuration du site concentrateur

Lors de la configuration du site concentrateur, vous créez deux stratégies VPN pour le site concentrateur simultanément, par exemple la stratégie VPN HubToSpoke1 et HubToSpoke2 en même temps. Pour configurer le concentrateur, saisissez les informations suivantes :

ÉTAPE 1 Sur la page **Advanced VPN Setup**, dans la **Table VPN Policy**, cliquez sur **Add Row**.

ÉTAPE 2 Pour configurer les paramètres VPN du site concentrateur, configurez les fonctions suivantes :

Add/Edit VPN Policy Configuration > Policy Name	Saisissez **HubToSpoke1** ou **HubToSpoke2**
Policy Type	Sélectionnez **Auto Policy** dans la liste déroulante.
VPN Failover	Laissez cette case décochée.
Interface	Sélectionnez l'interface Internet dans la liste déroulante.
Remote Endpoint	Sélectionnez **IP Address** dans la liste déroulante et saisissez l'adresse IP.
Redundant Enable	Laissez cette case décochée.
NetBIOS	Laissez cette case décochée.
Local Traffic Section > Local IP	Sélectionnez **Subnet** dans la liste déroulante.
IP Address	Saisissez le sous-réseau LAN local, par exemple **192.168.1.0** et **192.168.74.0** pour HubToSpoke1 ou **192.168.1.0** et **192.168.75.0** pour HubToSpoke2.
Subnet Netmask	Saisissez **255.255.255.0**, puis cliquez sur Add pour saisir l'adresse dans le champ **IP/Subnet List**.
Remote Traffic Section > Remote IP	Sélectionnez Subnet dans la liste déroulante.

IP Address	Saisissez le sous-réseau LAN distant, par exemple **192.168.75.0** pour HubToSpoke1 ou **192.168.74.0** pour HubToSpoke2.
Subnet Netmask	Saisissez **255.255.255.0**, puis cliquez sur Add pour saisir l'adresse dans le champ **IP/Subnet List**.

ÉTAPE 3 Cliquez sur **Save**.

Configuration du site spoke

Lors de la configuration du site spoke, vous devez créer une stratégie VPN pour chaque site spoke, par exemple la stratégie VPN Spoke1ToHub pour le site spoke1 et Spoke2ToHub pour le site spoke2. Pour configurer le site spoke, saisissez les informations suivantes :

ÉTAPE 1 Sur la page **Advanced VPN Setup**, dans la **Table VPN Policy**, cliquez sur **Add Row**.

Pour configurer les paramètres VPN de chaque site spoke, configurez les fonctions suivantes :

Add/Edit VPN Policy Configuration > Policy Name	Saisissez **Spoke1ToHub** ou **Spoke2toHub**.
Policy Type	Sélectionnez **Auto Policy** dans la liste déroulante.
VPN Failover	Laissez cette case décochée.
Interface	Sélectionnez l'interface Internet dans la liste déroulante.
Remote Endpoint	Sélectionnez **IP Address** dans la liste déroulante et saisissez l'adresse IP.
Redundant Enable	Laissez cette case décochée.
NetBIOS	Laissez cette case décochée.
Local Traffic Section > Local IP	Sélectionnez **Subnet** dans la liste déroulante.
IP Address	Saisissez le sous-réseau LAN local, par exemple **192.168.75.0** pour Spoke1ToHub ou **192.168.74.0** pour Spoke2ToHub.

Subnet Netmask	Saisissez **255.255.255.0**, puis cliquez sur Add pour saisir l'adresse dans le champ **IP/Subnet List**.
Remote Traffic Section > Remote IP	Sélectionnez **Subnet** dans la liste déroulante.
IP Address	Saisissez le sous-réseau LAN distant, par exemple **192.168.1.0 et 192.168.74.0** pour Spoke1ToHub ou **192.168.1.0** et **192.168.75.0** pour Spoke2ToHub.
Subnet Netmask	Saisissez **255.255.255.0**, puis cliquez sur **Add** pour saisir l'adresse dans le champ **IP/Subnet List**.

ÉTAPE 2 Cliquez sur **Save**.

ÉTAPE 3 Le sous-réseau 192.168.75.0/24 sur Spoke1 peut maintenant communiquer avec le sous-réseau 192.168.74.0/24 sur Spoke2 via Hub.

Gestion des certificats

Un certificat numérique certifie la propriété d'une clé publique par l'objet nommé du certificat. Cela permet à des tiers (aux parties utilisatrices) d'utiliser les signatures ou les assertions faites par la clé privée correspondant à la clé publique certifiée. Dans ce modèle de relations d'approbation, une autorité de certification (CA) est une partie tierce de confiance validée par l'objet (le propriétaire) du certificat et la partie utilisatrice du certificat. Les autorités de certification sont caractéristiques de nombreux systèmes d'infrastructure à clé publique (PKI).

La table comporte un certificat local auto-signé par défaut. Tous les certificats CA et certificats locaux importés, ainsi que la demande CSR générée, sont également affichés dans la table. Le certificat local par défaut est auto-signé et peut être exporté, mais pas supprimé. Il est uniquement utilisé via l'accès à l'IUG HTTPS. Tous les autres certificats locaux peuvent être supprimés et exportés. Les certificats CA peuvent être supprimés, mais pas exportés. Les demandes CSR peuvent être supprimées et exportées. La colonne « Action » inclut également un bouton « Import » pour les demandes CSR. Ce dernier permet d'importer le certificat local que la CA émet sur la base de cette demande CSR.

Utilisez la gestion des certificats pour générer et installer des certificats SSL.

Pour importer un certificat :

ÉTAPE 1 Sélectionnez **VPN > Certificate Management**. Dans la table **Certificate Management**, cliquez sur **Import Certificate**.

ÉTAPE 2 Sélectionnez **Import CA** ou **Import Local Certificate**.

ÉTAPE 3 Recherchez le certificat. Les routeurs RV132W/RV134W ne prennent en charge que les certificats au format PEM. Assurez-vous que le format du certificat est PEM et que le nom d'extension du fichier est .pem.

ÉTAPE 4 Cliquez sur **Start Upload.**

ÉTAPE 5 Cliquez sur **Save**.

Générateur de certificat

Le générateur de demande de certificat collecte des informations et génère un fichier de clé privée ainsi qu'une demande de certificat. Vous pouvez, si vous le souhaitez, générer un certificat auto-signé ou une demande de signature de certificat (CSR) pour une autorité de certification externe à signer.

Pour générer un certificat :

ÉTAPE 1 Sélectionnez **VPN > Certificate Management**. Dans la table **Certificate Management**, cliquez sur **Generate CSR**.

ÉTAPE 2 Saisissez les paramètres suivants :

- **Certificate Name** : nom du certificat.
- **Country Name** : nom du pays d'origine.
- **State or Province Name** : nom du département ou de la région (facultatif).
- **Locality Name** : municipalité (facultatif).
- **Organization Name** : organisation (facultatif).
- **Organizational Unit Name** : sous-groupe de l'organisation.
- **Common Name** : nom courant de l'organisation.
- **Key Encryption Length** : longueur de la clé.
- **IP Address** : adresse IP (facultatif). Pour utiliser l'adresse IP WAN local en tant qu'identifiant local, saisissez la valeur de l'adresse IP du WAN local à cet emplacement.

- **Domain Name** : nom du domaine (facultatif). Pour utiliser le nom de domaine complet en tant qu'identifiant local, saisissez la valeur du nom de domaine complet à cet emplacement.
- **Email Address** : adresse e-mail du contact (facultatif). Pour utiliser le nom de domaine complet de l'utilisateur en tant qu'identifiant local, saisissez la valeur du nom de domaine complet de l'utilisateur à cet emplacement.

ÉTAPE 3 Cliquez sur **Save**.

Configuration du protocole PPTP

Le protocole PPTP (Point to Point Tunneling Protocol) est un protocole réseau qui permet de transférer en toute sécurité des données depuis un client distant vers un réseau d'entreprise en créant une connexion VPN sécurisée sur les réseaux publics, comme Internet.

Configuration du serveur PPTP

Pour configurer le serveur VPN PPTP (pour le modèle RV134W uniquement) :

ÉTAPE 1 Sélectionnez **VPN > PPTP Server**.

ÉTAPE 2 Dans PPT Configuration, saisissez les informations suivantes.

a. Dans le champ PPTP Server, cochez la case **Enable**.

b. Saisissez l'adresse IP du serveur PPTP.

c. Saisissez la plage d'adresses IP pour les clients PPTP.

d. Pour crypter les données transitant par la connexion VPN PPTP, cochez la case **Enable** pour activer **MPPE Encryption**. Le cryptage MPPE pour la prise en charge du serveur PPTP est de 128 bits.

ÉTAPE 3 Cliquez sur **Save**.

Création et gestion des utilisateurs PPTP

Pour créer et activer les utilisateurs PPTP :

ÉTAPE 1 Dans la **table VPN Client Setting,** cliquez sur **Add Row**.

ÉTAPE 2 Saisissez le nom d'utilisateur et le mot de passe permettant d'authentifier l'utilisateur PPTP. Saisissez des valeurs comprises entre 1 et 64 caractères.

ÉTAPE 3 Cochez la case **Enable** pour activer le compte d'utilisateur.

ÉTAPE 4 Cliquez sur le bouton Import pour accéder à la page de configuration de l'utilisateur (dans le menu Administration > Users). Au bas de la page, importez le fichier .csv avec les paires nom d'utilisateur/mot de passe.

ÉTAPE 5 Cliquez sur **Save.**

Configuration de l'intercommunication VPN

L'intercommunication VPN permet au trafic VPN provenant des clients VPN de transiter par le routeur.

Pour configurer l'intercommunication VPN :

ÉTAPE 1 Sélectionnez VPN > **VPN Passthrough.**

ÉTAPE 2 Cochez la case **Enable** pour choisir le type de trafic autorisé à transiter par l'appareil.

ÉTAPE 3 Cliquez sur **Save**.

7

Qualité de service (QoS)

Les paramètres de qualité de service (QoS) attribuent une priorité à différents utilisateurs, applications ou flux de données ou garantissent un certain niveau de performances sur un flux de données. Ces garanties sont importantes lorsque la capacité du réseau est insuffisante, notamment pour les applications multimédias de diffusion en temps réel, telles que la voix sur IP, les jeux en ligne et la télévision IP. En effet, ces applications nécessitent un débit fixe et sont sensibles aux retards. Il en va de même sur les réseaux dont la capacité est assurée par une ressource limitée.

Gestion de la bande passante

Vous pouvez utiliser la fonction de gestion de la bande passante du routeur pour gérer la bande passante du trafic entre le réseau sécurisé (LAN) et le réseau non sécurisé (WAN).

Configuration de la bande passante

Vous pouvez limiter la bande passante afin de réduire le débit de transmission de données du routeur. Vous pouvez également utiliser un profil de bande passante pour limiter le trafic sortant afin d'empêcher les utilisateurs du réseau LAN de consommer toute les bandes passantes de la liaison Internet.

Pour définir la bande passante amont :

ÉTAPE 1 Sélectionnez **QoS > Bandwidth Management**.

ÉTAPE 2 Dans le champ WAN QoS de la section Global Settings, cochez la case **Enable**.

ÉTAPE 3 Dans la **table Bandwidth**, saisissez la bande passante amont que vous souhaitez allouer à chacune des interfaces disponibles :

Upstream	Bande passante (en Kbit/s) utilisée pour envoyer des données sur Internet.

ÉTAPE 4 Cliquez sur **Save**.

Configuration de la stratégie de liaison QoS

Dans la table QoS Binding, vous pouvez configurer la stratégie QoS pour le trafic amont.

ÉTAPE 1 Cliquez sur **Add Row**.

ÉTAPE 2 Saisissez les informations dans les champs suivants pour ajouter ou modifier les paramètres de la stratégie :

Policy Name	Nom de la stratégie.
Protocol	Sélectionnez le protocole dans la liste déroulante (TCP et UCP, TCP ou UCP).
Source Port	Sélectionnez le port source dans la liste déroulante. Il peut s'agir de n'importe quel port, d'un port unique ou d'une plage de ports.
Destination Port	Sélectionnez le port de destination dans la liste déroulante. Il peut s'agir de n'importe quel port, d'un port unique ou d'une plage de ports.
Source IP	Sélectionnez l'adresse IP source dans la liste déroulante. Il peut s'agir de n'importe quelle adresse IP, d'une adresse IP unique ou d'une plage d'adresses IP.
Destination IP	Sélectionnez l'adresse IP de destination dans la liste déroulante. Il peut s'agir de n'importe quelle adresse IP, d'une adresse IP unique ou d'une plage d'adresses IP.

MAC Address	Sélectionnez le type d'adresse MAC dans la liste déroulante. Il peut s'agir de **n'importe quelle** adresse ou d'une adresse **MAC unique**. Il s'agit de l'adresse MAC de la source de ce trafic.
VLAN ID	Sélectionnez l'**ID VLAN** dans la liste déroulante. Il s'agit de l'ID VLAN de la source de ce trafic.
Available SSIDs	Sélectionnez les **SSID** disponibles dans la liste déroulante. Il s'agit du SSID de la source de ce trafic.
Physical Port	Sélectionnez le port (**1-3 pour RV132W** ou **1- 4 pour RV134W**) dans la liste déroulante. Il s'agit du port VLAN de la source de ce trafic.
Queue	Définissez la priorité (**1 étant la plus basse et 4 la plus élevée)** pour la catégorie sélectionnée.
Rate Limit (Kbit/Sec) :	Saisissez le débit maximal en kilobits par seconde.
Remarking	Cochez la case **Enable** pour activer le remarquage sur la classe de service (CoS) ou sur DSCP (Differentiated Services Code Point).
CoS ou DSCP	Saisissez la valeur de remarquage pour les paquets de ce réseau.

ÉTAPE 3 Cliquez sur **Save**.

Pour modifier les paramètres d'une entrée dans la table, cochez la case correspondante, puis cliquez sur **Edit**. Une fois les modifications terminées, cliquez sur **Save**.

Pour supprimer une entrée de la table, cochez la case correspondante, puis cliquez sur **Delete**. Cliquez sur **Save**.

Configuration des paramètres de port QoS

Vous pouvez configurer les paramètres QoS pour chaque port de votre appareil. Ce dernier prend en charge quatre files d'attente de priorité permettant de définir la priorité du trafic pour chaque port.

Pour configurer les paramètres QoS des ports de votre appareil :

ÉTAPE 1 Sélectionnez **QoS** > **QoS Port-Based Settings**.

ÉTAPE 2 Pour chaque port de la table **QoS Port-Based Settings**, saisissez les informations suivantes :

Trust Mode	Sélectionnez l'une des options suivantes dans le menu déroulant : ▪ **Port** : active les paramètres de port QoS. Vous pouvez alors définir la priorité du trafic pour un port particulier. La priorité de la file d'attente de trafic commence avec le niveau de priorité le plus faible (1) et finit avec le niveau de priorité le plus élevé (4). ▪ **DSCP** : DSCP (Differentiated Services Code Point, point de code de services différenciés). L'activation de cette fonctionnalité privilégie le trafic réseau d'après la mise en correspondance de la file d'attente DSCP sur la page **DSCP Settings**. ▪ **CoS** : classe de service (Class of Service). L'activation de cette fonctionnalité privilégie le trafic réseau d'après la mise en correspondance de la file d'attente CoS sur la page **CoS Settings**.
File d'attente de transfert du trafic par défaut pour les appareils non validés	Sélectionnez un niveau de priorité pour le trafic sortant (de 1 à 4).

ÉTAPE 3 Cliquez sur **Save**.

Pour rétablir les paramètres de port QoS par défaut, cliquez sur **Restore Default**, puis enregistrez vos modifications.

Configuration des paramètres CoS

Utilisez le lien vers la page QoS Port-Based Settings pour mettre en correspondre le paramètre de priorité CoS avec la file d'attente QoS.

Pour mettre en correspondance les paramètres de priorité CoS avec la file d'attente de redirection du trafic :

ÉTAPE 1 Sélectionnez **QoS** > **CoS Settings**.

ÉTAPE 2 Pour chaque niveau de priorité CoS dans la **table CoS Settings**, sélectionnez une valeur de priorité dans le menu déroulant **Traffic Forwarding Queue**.

Ces valeurs associent aux différents types de trafic des niveaux de priorité plus ou moins élevés.

ÉTAPE 3 Cliquez sur **Save**.

Pour rétablir les paramètres de port QoS par défaut, cliquez sur **Restore Default**, puis sur **Save**.

Configuration des paramètres DSCP

Vous pouvez configurer la mise en correspondance des files d'attente DSCP et QoS depuis la page **DSCP Settings**.

Pour configurer la mise en correspondance des files d'attente DSCP et QoS :

ÉTAPE 1 Sélectionnez **QoS** > **DSCP Settings**.

ÉTAPE 2 Choisissez de répertorier uniquement les valeurs RFC ou toutes les valeurs DSCP dans la **table DSCP Settings** en cliquant sur le bouton correspondant.

ÉTAPE 3 Pour chaque valeur DSCP de la **table DSCP Settings**, sélectionnez un niveau de priorité dans le menu déroulant **Queue**.

La valeur DSCP est alors mise en correspondance avec la file d'attente QoS sélectionnée.

ÉTAPE 4 Cliquez sur **Save**.

Pour rétablir les paramètres DSCP par défaut, cliquez sur **Restore Default** et sur **Save**.

8

Administration

Complexité des mots de passe

La sécurité et la complexité des mots de passe est une mesure préventive qui permet de contrer les attaques de décryptage et en force brute. La sécurité d'un mot de passe dépend de la longueur, de la complexité et de l'imprévisibilité.

L'utilisation de mots de passe forts réduit le risque global d'une faille de sécurité. Vous pouvez exiger une complexité minimale du mot de passe lors des changements de mot de passe.

Pour configurer les paramètres de complexité du mot de passe :

ÉTAPE 1 Sélectionnez **Administration** > **Password Complexity**.

ÉTAPE 2 Dans le champ **Password Complexity Enforcement**, cochez la case **Enable**.

ÉTAPE 3 Configurez les paramètres de complexité du mot de passe :

Minimum password length	Saisissez la longueur minimale du mot de passe (entre 0 et 32 caractères).
Maximum password length	Saisissez la longueur maximale du mot de passe (entre 64 et 80 caractères).
Minimum number of character classes	Saisissez un nombre correspondant à l'une des catégories de caractères suivantes : ▪ Lettres majuscules. ▪ Lettres minuscules. ▪ Chiffres. ▪ Les caractères spéciaux sont disponibles sur un clavier standard. Par défaut, les mots de passe doivent contenir des caractères d'au moins trois de ces catégories.

The new password must be different than the current one	Cochez la case **Enable** pour exiger que les nouveaux mots de passe soient différents du mot de passe actuel.
Enforce Password Aging	Cochez la case **Enable** pour que les mots de passe expirent après un délai donné.
Maximum Password Age	Saisissez le nombre de jours au bout duquel le mot de passe expire (1–365). La valeur par défaut est de 180 jours.

ÉTAPE 4 Cliquez sur **Save**.

Configuration des comptes d'utilisateurs

Votre routeur prend en charge deux comptes d'utilisateurs pour l'administration et l'affichage des paramètres : un administrateur (nom d'utilisateur et mot de passe par défaut : cisco) et un invité (nom d'utilisateur par défaut : guest).

Le compte invité (guest) est en lecture seule. Vous pouvez définir et modifier le nom d'utilisateur et le mot de passe des comptes administrateur et invité.

Configuration des comptes d'utilisateurs

Pour configurer les comptes d'utilisateurs :

ÉTAPE 1 Sélectionnez **Administration** > **Users**.

ÉTAPE 2 Dans le champ **Account Activation**, cochez les cases des comptes que vous souhaitez activer (le compte administrateur doit être actif).

ÉTAPE 3 (Facultatif) Pour modifier le compte administrateur, sous **Administrator Account Setting,** cochez **Edit Administrator Settings**. Pour modifier le compte invité, sous Guest Settings, cochez **Edit Guest Settings**. Saisissez les informations suivantes :

New Username	Saisissez un nouveau nom d'utilisateur.
Old Password	Saisissez le mot de passe actuel.

New Password	Saisissez le nouveau mot de passe. Nous vous recommandons d'utiliser un mot de passe qui ne contienne aucun mot figurant dans un dictionnaire, quelle que soit la langue, et qui soit composé de lettres (majuscules et minuscules), de chiffres et de symboles. Le mot de passe peut comporter jusqu'à 64 caractères.
Retype New Password	Saisissez une nouvelle fois le nouveau mot de passe.

ÉTAPE 4 Cliquez sur **Save**.

Importation de comptes d'utilisateurs

Vous pouvez importer simultanément plusieurs utilisateurs à l'aide d'un fichier CSV.

Assurez-vous que les données du fichier CSV apparaissent comme dans les tableaux suivants :

TYPE	NOM D'UTILISATEUR	MOT DE PASSE
Admin	Admin123	Admin123
Invité	Guest123	Guest123

TYPE	NOM D'UTILISATEUR	MOT DE PASSE	ACTIVATION
PPTP	PPTP-user-1	12345678	activer
PPTP	PPTP-user-2	345123678	désactiver

REMARQUE : Les noms des colonnes respectent la casse. Ne changez pas l'ordre des noms des colonnes.

Pour importer des comptes d'utilisateurs à partir d'un fichier CSV :

ÉTAPE 1 Dans le champ **Import User Name & Password**, cliquez sur **Browse**.

ÉTAPE 2 Recherchez le fichier et cliquez sur **Open**.

ÉTAPE 3 Cliquez sur **Import**.

ÉTAPE 4 Cliquez sur **Save**.

REMARQUE : Vous pouvez télécharger la grille utilisateur pour créer votre propre liste de noms d'utilisateurs et de mots de passe. Pour télécharger la grille, cliquez sur **Download** dans le champ **Download User template**.

Configuration du délai d'expiration de session

Le délai d'expiration est le nombre de minutes d'inactivité autorisées avant la fermeture de la session du Gestionnaire de périphérique. Vous pouvez configurer le délai d'expiration pour les comptes administrateur et invité.

Pour configurer le délai d'expiration de la session :

ÉTAPE 1 Sélectionnez **Administration** > **Session Timeout**.

ÉTAPE 2 Dans le champ **Web Administrator Inactivity Timeout**, saisissez le nombre de minutes avant l'expiration d'une session pour cause d'inactivité. Sélectionnez **Never** pour permettre à l'administrateur de rester connecté en permanence.

ÉTAPE 3 Dans le champ **Web Guest Inactivity Timeout**, saisissez le nombre de minutes avant l'expiration d'une session pour cause d'inactivité. Sélectionnez **Never** pour permettre à l'administrateur de rester connecté en permanence.

ÉTAPE 4 Dans le champ **SSH Inactivity Timeout**, saisissez le nombre de minutes avant l'expiration d'une session pour cause d'inactivité. Sélectionnez **Never** pour permettre à l'administrateur de rester connecté en permanence.

ÉTAPE 5 Cliquez sur **Save**.

Texte de la bannière de connexion

Les bannières de connexion (pour l'interface de ligne de commande [CLI] uniquement) présentent un avertissement aux intrus susceptibles de vouloir accéder à votre système. Ils confirment que certains types d'activités sont interdits et informent les utilisateurs autorisés de leurs obligations concernant l'utilisation acceptable des environnements en réseau.

Pour mettre à jour les champs **Pre-Login Banner Text**, saisissez le texte de la bannière de connexion dans la zone de texte. Celui-ci est affiché dans l'interface de ligne de commande avant la connexion de l'utilisateur.

Pour mettre à jour les champs **Post-Login Banner Text**, saisissez le texte de la bannière de connexion dans la zone de texte. Celui-ci est affiché dans l'interface de ligne de commande après la connexion de l'utilisateur.

Configuration des paramètres TR-069

Le TR-069 est une spécification pour le protocole CWMP (CPE WAN Management Protocol) définie par le DSL Forum. Il s'agit d'un protocole de gestion des communications entre la couche d'application et les terminaux des utilisateurs. Ce protocole SOAP/HTTP bidirectionnel assure la communication entre l'équipement sur le site client (CPE) et les serveurs à configuration automatique (ACS).

REMARQUE : Le TR069 et l'interface utilisateur graphique ne peuvent pas être gérés simultanément. Après avoir configuré le TR069 et enregistré les paramètres, déconnectez-vous de l'interface utilisateur graphique Web. Le CPE peut ensuite établir la connexion à l'ACS.

Pour configurer les paramètres TR-069 :

ÉTAPE 1 Cliquez sur Administration > **TR-069 Settings**. La page **TR-069 Settings** s'ouvre.

ÉTAPE 2 Dans la zone **TR-069 Settings**, cliquez sur **Enable** pour activer le client TR-069 ou sur **Disable** pour le désactiver.

ÉTAPE 3 Dans la zone **IP Protocol**, sélectionnez le protocole **IPv4** ou **IPv6**.

ÉTAPE 4 Dans la zone **Inform**, cochez la case **Enable** pour activer l'option ou la case **Disable** pour la désactiver.

ÉTAPE 5 Dans le champ **Inform Interval**, saisissez le nombre de secondes (la valeur par défaut est 300).

ÉTAPE 6 Dans la zone **ACS**, indiquez les paramètres du serveur de gestion à distance ACS :

- **ACS URL :** Dans la liste déroulante ACS URL, sélectionnez le protocole ACS URL (HTTP:// ou HTTPS://) et saisissez l'URL.
- **ACS Username :** saisissez le nom d'utilisateur de connexion au serveur de gestion à distance ACS.
- **ACS Password :** saisissez le mot de passe de connexion au serveur de gestion à distance ACS.
- Si le protocole https est sélectionné, renseignez les informations suivantes :
- **ACS side CA certificate file import :** cliquez pour importer le contenu du fichier de certificat CA validé.
- **ACS side CA certificate file show** : cliquez pour afficher la liste de certificats CA validés.
- **ACS certificate file select** : cliquez pour sélectionner la liste déroulante de CA validés.
- **CPE certificate file import** : cliquez pour importer le contenu du fichier de certificat CA CPE.
- **CPE certificate file show** : cliquez pour afficher la liste de certificats CA CPE.
- **CPE certificate file select** : cliquez pour sélectionner la liste déroulante de CA CPE.

ÉTAPE 7 Dans la section **Display SOAP messages de la console série,** cochez la case **Enable** pour afficher les messages SOAP ou la case **Disable** pour les désactiver.

ÉTAPE 8 **Download Request :** (facultatif) indiquez le type de demande de téléchargement, puis cliquez sur **Send** pour envoyer la requête de téléchargement correspondante au serveur TR-069.

- **Firmware :** demander le téléchargement du microprogramme des routeurs RV132W/RV134W à partir du serveur TR-069.
- **Vendor Configuration :** demander le téléchargement du fichier de configuration à partir du serveur TR-069.

ÉTAPE 9 Cochez la case **Connection Request Authentication** et saisissez les informations suivantes :

- **Username :** saisissez le nom d'utilisateur pour vous connecter via l'authentification de la demande de connexion.
- **Password :** saisissez le mot de passe pour vous connecter via l'authentification de la demande de connexion.
- **Connection Request port** : saisissez le port de la demande de connexion. Par défaut, il s'agit du port 7547.

ÉTAPE 10 Dans le champ **Bind Interface**, sélectionnez **Auto** pour lier le service TR-069 à l'interface active actuelle, ou sélectionnez l'une des interfaces auxquelles le lier. Cliquez sur **Save** pour enregistrer vos paramètres.

ÉTAPE 11 Cliquez sur **Export Data Model** pour exporter le modèle TR-069 de l'appareil.

Diagnostics

Votre routeur fournit plusieurs outils de diagnostic pour vous aider à résoudre des problèmes de réseau.

Outils réseau

Exécutez les utilitaires de diagnostic suivants pour accéder à la configuration des routeurs RV132W/RV134W et surveillez l'intégrité globale du réseau.

Utilisation de l'utilitaire Ping ou Traceroute

Vous pouvez exécuter l'utilitaire Ping ou Traceroute pour tester la connectivité entre ce routeur et un autre périphérique du réseau. Pour utiliser Ping ou Traceroute :

ÉTAPE 1 Sélectionnez **Administration > Diagnostics > Network Tools**.

ÉTAPE 2 Dans le champ **IP Address / Domain Name**, saisissez l'adresse IP de l'appareil ou un nom de domaine complet, comme www.cisco.com, que vous souhaitez soumettre au test ping.

ÉTAPE 3 Cliquez sur **Ping**. Les résultats de la requête ping s'affichent. Ces résultats indiquent si l'appareil est accessible. Vous pouvez également cliquer sur **Traceroute**. Les résultats Traceroute s'affichent.

Recherche DNS

Vous pouvez utiliser l'outil de recherche pour trouver l'adresse IP de l'hôte (par exemple, un serveur Web, FTP ou de messagerie) sur Internet.

Pour récupérer l'adresse IP d'un serveur Web, FTP, de messagerie ou de tout autre serveur sur Internet, saisissez le nom Internet dans la zone de texte, puis cliquez sur **Look up**. Si l'hôte ou le domaine saisi existe, vous obtenez une réponse contenant l'adresse IP. Le message Unknown Host indique que le nom Internet spécifié n'existe pas.

Pour utiliser l'outil de recherche :

ÉTAPE 1 Sélectionnez **Administration > Diagnostics > Network Tools**.

ÉTAPE 2 Dans le champ **Internet Name**, saisissez le nom Internet de l'hôte.

ÉTAPE 3 Cliquez sur **Look up**. Les résultats de la recherche s'affichent.

Capture des paquets

La capture de paquets est un terme du domaine des réseaux informatiques désignant l'interception d'un paquet de données qui traverse un réseau informatique spécifique ou transféré sur ce dernier.

Pour démarrer une capture de paquets, dans le menu déroulant **Select a layer 2 interface for this service**, sélectionnez votre type de connexion (LAN, DSL WAN ou ETH WAN).

- Cliquez sur **Start** pour démarrer la capture de paquets.
- Cliquez sur **Stop** pour interrompre la capture de paquets.
- Cliquez sur **Save packet log** pour enregistrer le journal de paquets.

ÉTAPE 4 **DSL Diagnostics**. Cliquez sur **Enable** pour activer les diagnostics DSL.

Mise en miroir des ports

La mise en miroir des ports surveille le trafic réseau en envoyant des copies de tous les paquets entrants et sortants d'un port à un port de surveillance. La mise en miroir des ports peut servir d'outil de diagnostic ou de débogage pour repousser une attaque ou surveiller le trafic utilisateur de LAN à WAN afin de déterminer si les utilisateurs accèdent à des informations ou à des sites Web inappropriés.

L'hôte LAN (PC) doit utiliser une adresse IP statique pour éviter tout problème avec la mise en miroir des ports. Les baux DHCP d'un hôte LAN peuvent expirer et entraîner l'échec de la mise en miroir des ports si une adresse IP statique n'est pas configurée pour l'hôte LAN.

Pour configurer la mise en miroir des ports :

ÉTAPE 1 Sélectionnez **Administration** > **Diagnostics** > **Port Mirroring**.

ÉTAPE 2 Dans le menu déroulant **Mirror Destination Port**, sélectionnez un port miroir. Si vous utilisez un port pour la mise en miroir, ne l'utilisez pas pour d'autres types de trafic.

ÉTAPE 3 Dans le champ **Mirror Source Port**, sélectionnez les ports à mettre en miroir.

ÉTAPE 4 Cliquez sur **Save**.

Paramètres de la clé de support distante

La clé de support est utilisée par les techniciens du support technique Cisco pour obtenir de plus amples informations sur l'appareil pendant le dépannage. La clé par défaut est « **key001** ». Incluez la clé lorsque vous faites une demande d'assistance auprès de Cisco et que vous souhaitez que le technicien de support technique accède à votre routeur à distance. Pour configurer une clé de support à distance, saisissez le nom de la clé dans le champ **Remote Support Key**.

Configuration de la journalisation

Configurez les journaux pour surveiller l'activité indiquant l'état de fonctionnement et de performance de votre appareil.

Configuration des paramètres de journal

Pour configurer la journalisation :

ÉTAPE 1 Sélectionnez **Administration > Logging > Log Settings**.

ÉTAPE 2 Dans le champ **Log Mode**, cochez la case **Enable**.

ÉTAPE 3 Cliquez sur **Add Row**.

ÉTAPE 4 Configurez les paramètres suivants :

Remote Log Server	Saisissez l'adresse IP du serveur de journalisation qui enregistrera les journaux.
Log Severity	Sélectionnez la gravité des événements pour lesquels vous souhaitez enregistrer les journaux et les envoyer à une adresse e-mail/de serveur spécifique. Tous les types de journaux dont la gravité est supérieure à celle du type de journal sélectionné sont automatiquement inclus et ne peuvent pas être exclus. Par exemple, si vous sélectionnez les journaux Error, alors Emergency, Alert et Critical sont également sélectionnés. Les niveaux de gravité des événements sont répertoriés du plus élevé au plus faible, comme suit : ▪ **Emergency** : le système n'est pas utilisable. ▪ **Alert** : une action est requise. ▪ **Critical** : le système est dans un état critique. ▪ **Error** : le système subit une condition d'erreur. ▪ **Warning** : un avertissement système a été généré. ▪ **Notification** : le système fonctionne correctement, mais une notification système a été générée. ▪ **Information** : informations sur l'appareil. ▪ **Debugging** : informations détaillées sur un événement. La sélection de ce niveau de gravité des journaux entraîne la génération de grandes quantités de journaux et n'est pas recommandée dans le cadre d'un fonctionnement normal du routeur.
Enable	Cochez la case **Enable** pour activer les paramètres de journalisation.

ÉTAPE 5 Cliquez sur **Save**.

ÉTAPE 6 Cliquez sur **View Logs** pour afficher la table des journaux système.

Pour modifier une entrée dans la **Table Logging Setting**, sélectionnez l'entrée en question, puis cliquez sur **Edit**. Apportez les modifications souhaitées, puis cliquez sur **Save**.

Configuration des paramètres d'e-mail

Vous pouvez configurer votre appareil afin qu'il envoie les journaux par e-mail. Nous vous recommandons de configurer un compte de messagerie distinct pour l'envoi et la réception des journaux.

Vous devez commencer par configurer la sévérité des journaux à capturer ; voir la section **Configuration des paramètres de journal**.

Pour configurer l'envoi des journaux par e-mail :

ÉTAPE 1 Sélectionnez **Administration** > **Logging** > **E-mail Settings**.

ÉTAPE 2 Pour activer les journaux par e-mail, cochez la case **Enable**.

La gravité minimale des journaux à capturer s'affiche. Pour la modifier, cliquez sur **Configure Severity**.

ÉTAPE 3 Configurez les paramètres suivants :

E-mail Server Address	Saisissez l'adresse du serveur SMTP. Il s'agit du serveur de messagerie associé au compte de messagerie que vous avez configuré (par exemple, mail.nom_entreprise.com).
E-mail Server Port	Saisissez le port du serveur SMTP. Si votre fournisseur de messagerie demande un port spécial pour le courrier électronique, entrez-le à cet emplacement. Dans le cas contraire, utilisez la valeur par défaut (25).
Return E-mail Address	Saisissez l'adresse e-mail de retour à laquelle l'appareil enverra les messages si les journaux provenant du routeur et acheminés à l'adresse e-mail de destination ne peuvent pas être remis.

Send to E-mail Address 1, (Address 2, facultatif), (Address 3, facultatif)	Saisissez une adresse e-mail à laquelle envoyer les journaux (par exemple, logging@nom_entreprise.com).
E-mail Encryption	Sélectionnez **SSL** ou **TSL** comme méthode de cryptage e-mail. Sélectionnez **Enable** pour utiliser une méthode de cryptage e-mail.
Authentication with SMTP Server	Si le serveur (de messagerie) SMTP exige une authentification avant d'accepter les connexions, sélectionnez le type d'authentification dans le menu déroulant : **None**, **LOGIN**, **PLAIN** et **CRAM-MD5**.
E-mail Authentication Username	Saisissez le nom d'utilisateur d'authentification e-mail (par exemple, *logging@nom_entreprise.com*).
E-mail Authentication Password	Saisissez le mot de passe d'authentification e-mail (par exemple, le mot de passe utilisé pour accéder au compte de messagerie que vous avez configuré pour l'envoi des journaux).
E-mail Test	Cliquez sur **Test** pour tester l'authentification e-mail.

ÉTAPE 4 Dans la section **Send E-Mail Logs by Schedule**, configurez les paramètres suivants :

Unit	Sélectionnez l'unité de temps pour les journaux (**Never**, **Hourly**, **Daily** ou **Weekly**). Si vous sélectionnez **Never**, les journaux ne sont pas envoyés.
Day	Si vous choisissez une fréquence d'envoi hebdomadaire des journaux, sélectionnez le jour de la semaine auquel envoyer les journaux.
Time	Si vous choisissez une fréquence d'envoi des journaux (quotidienne ou hebdomadaire), sélectionnez l'heure de la journée à laquelle envoyer les journaux.

ÉTAPE 5 Dans la section Email Alert, configurez les paramètres suivants :

Email alert when WAN up/down	Cochez la case **Enable** pour recevoir une alerte par e-mail lorsque le réseau WAN est actif ou inactif.
Email alert when VPN up/down	Cochez la case **Enable** pour recevoir une alerte par e-mail lorsque le VPN est actif ou inactif.

ÉTAPE 6 Cliquez sur **Save**.

Configuration de Discovery Bonjour

Discovery Bonjour est un protocole de découverte et d'annonce de service. Sur votre appareil, Bonjour n'annonce les services par défaut configurés sur l'appareil que s'il est activé.

Pour activer Discovery Bonjour :

ÉTAPE 1 Sélectionnez **Administration** > **Discovery Bonjour**.

ÉTAPE 2 Cochez la case **Activer** pour activer le protocole Bonjour.

ÉTAPE 3 Pour activer Bonjour pour un réseau VLAN répertorié dans la **Table Bonjour Interface Control**, cochez la case **Enable Bonjour** correspondante.

Vous pouvez activer Bonjour sur des réseaux VLAN spécifiques. L'activation de Bonjour sur un réseau VLAN permet aux périphériques sur le réseau VLAN de détecter les services Bonjour disponibles sur le routeur (tels que HTTP/HTTPS).

Par exemple, si un réseau VLAN est configuré avec un ID de 2, les appareils et les hôtes sur un réseau VLAN 2 ne peuvent pas découvrir les services Bonjour exécutés sur le routeur, à moins que Bonjour soit activé pour VLAN 2.

ÉTAPE 4 Cliquez sur **Save**.

Configuration des propriétés LLDP

LLDP est un protocole de détection du voisinage utilisé pour les périphériques réseau pour transmettre des informations les concernant sur le réseau. Ce protocole s'exécute sur la couche de liaison de données, qui permet à deux systèmes d'exécuter différents protocoles de couche réseau pour se renseigner mutuellement.

Pour activer les propriétés LLPD sur le routeur, procédez comme suit :

ÉTAPE 1 Sélectionnez **Administration > LLDP Properties.**

ÉTAPE 2 Cochez la case **Enable** pour activer les options suivantes : LLPD status, DSL_ATM_WAN_0_33_R, ETH_WAN_R, DSL_PTM_WAN_1_1_R, IP_USB, PPP_USB.

ÉTAPE 3 Cliquez sur **Save**.

Configuration des paramètres d'heure

Vous pouvez configurer votre fuseau horaire, indiquer s'il faut ou non prendre en compte l'heure d'été et définir le serveur NTP (Network Time Protocol) avec lequel synchroniser la date et l'heure. Le routeur obtient alors ses informations de date et d'heure du serveur NTP.

Pour configurer les paramètres NTP et d'heure :

ÉTAPE 1 Sélectionnez **Administration** > **Time Settings**. L'heure actuelle s'affiche.

ÉTAPE 2 Renseignez les champs suivants :

Time Zone	Sélectionnez votre fuseau horaire par rapport à l'heure de Greenwich (GMT).
Adjust for Daylight Savings Time	Si cela est pertinent pour votre zone géographique, cochez la case **Adjust for Daylight Savings Time**.
Daylight Saving Mode	Si vous sélectionnez **By date**, saisissez la date à laquelle le mode heure d'été doit démarrer. Si vous sélectionnez **Recurring**, saisissez le mois, la semaine, le jour de la semaine et l'heure de démarrage du mode heure d'été. Saisissez les informations appropriées dans les champs **From** et **To**.

Daylight Saving Offset	Dans le menu déroulant, sélectionnez le décalage par rapport au temps universel coordonné (UTC).
Set Date and Time	Indiquez si vous souhaitez que la date et l'heure soient définies manuellement ou automatiquement sur l'appareil.
NTP Server	Pour utiliser les serveurs NTP par défaut, cliquez sur le bouton **Use Default**. Pour utiliser un serveur NTP spécifique, cliquez sur **User Defined NTP Server** et saisissez le nom de domaine complet ou l'adresse IP du serveur NTP dans les deux champs disponibles.
Enter Date and Time	Si vous sélectionnez **Manuel**, saisissez la date et l'heure dans les champs **Enter Date and Time**.

ÉTAPE 3 Cliquez sur **Save**.

Téléchargement et sauvegarde du fichier de configuration

Vous pouvez sauvegarder les paramètres de configuration personnalisés en vue d'une restauration ultérieure, ou les restaurer depuis une précédente sauvegarde à partir de la page **Administration > Download/Backup Configuration File**.

Lorsque le pare-feu fonctionne tel que configuré, vous pouvez sauvegarder la configuration pour une restauration ultérieure. Lors de la sauvegarde, vos paramètres sont enregistrés sous la forme d'un fichier sur votre ordinateur. Vous pouvez restaurer les paramètres du pare-feu à partir de ce fichier.

AVERTISSEMENT Lors d'une restauration, n'essayez pas de naviguer en ligne, ne désactivez pas le pare-feu, n'arrêtez pas l'ordinateur et n'utilisez pas le pare-feu jusqu'au terme de l'opération. Celle-ci devrait prendre environ une minute. Lorsque le voyant de test s'éteint, patientez encore quelques secondes avant d'utiliser le pare-feu.

Sauvegarde des paramètres de configuration

Pour sauvegarder ou restaurer la configuration :

ÉTAPE 1 Sélectionnez **Administration** > **Download/Backup Configuration Settings**.

ÉTAPE 2 Sélectionnez la configuration dans les paramètres **Configuration Download & Clear** :

Startup configuration	Sélectionnez cette option pour télécharger la configuration de démarrage. La configuration de démarrage est la configuration de fonctionnement la plus couramment utilisée par l'appareil. En cas de perte de la configuration de démarrage du routeur, utilisez cette page pour copier la configuration de secours vers la configuration de démarrage et restaurer les informations de configuration antérieures. Vous pouvez télécharger la configuration de démarrage vers d'autres routeurs RV132/RV134W pour faciliter le déploiement.
Mirror configuration	Sélectionnez cette option si l'appareil doit sauvegarder la configuration de démarrage après 24 heures de fonctionnement sans aucune modification dans la configuration de démarrage.
Backup configuration	Sélectionnez cette option pour sauvegarder les paramètres de configuration actuels.

ÉTAPE 3 Pour télécharger un fichier de sauvegarde d'après l'option de configuration sélectionnée, cliquez sur **Download**.

Par défaut, le fichier (startup.cfg, mirror.cfg ou backup.cfg) est téléchargé dans le dossier Téléchargements par défaut ; par exemple, C:\Documents and Settings\admin\Mes documents\Téléchargements\.

ÉTAPE 4 Pour effacer la configuration sélectionnée, cliquez sur **Clear**.

Téléchargement de la configuration

Pour télécharger une configuration de démarrage ou de sauvegarde :

ÉTAPE 1 Sélectionnez **Administration > Download/Backup Configuration File**.

ÉTAPE 2 Dans le champ **Configuration Upload**, sélectionnez la configuration à charger (**Startup Configuration** ou **Backup Configuration**).

ÉTAPE 3 Cliquez sur **Browse** pour localiser le fichier.

ÉTAPE 4 Sélectionnez le fichier, puis cliquez sur **Open**.

ÉTAPE 5 Cliquez sur **Start to Upload**.

L'appareil charge le fichier de configuration et utilise les paramètres qu'il contient pour mettre à jour la configuration de démarrage. Puis, il redémarre et utilise la nouvelle configuration.

Copie des paramètres de configuration

Copiez la configuration de démarrage dans la configuration de secours pour être sûr de disposer d'une copie de secours si vous oubliez votre nom d'utilisateur et votre mot de passe et que vous ne parvenez plus à accéder au Gestionnaire de périphérique. Pour revenir au Gestionnaire de périphérique, rétablissez les valeurs par défaut du périphérique.

Le fichier de Configuration de secours reste en mémoire et permet de copier les informations de configuration sauvegardées vers la Configuration de démarrage, qui restaure l'ensemble des paramètres.

Pour copier une configuration (par exemple, pour copier une configuration de démarrage vers la configuration de secours) :

ÉTAPE 1 Sélectionnez **Administration > Download/Backup Configuration File**.

ÉTAPE 2 Dans le champ **Copy**, sélectionnez les configurations source et de destination dans les menus déroulants.

ÉTAPE 3 Cliquez sur **Start to Copy**.

Génération d'une clé de cryptage

Le routeur vous permet de générer une clé de cryptage pour protéger les fichiers de secours.

Pour générer une clé de cryptage :

ÉTAPE 1 Sélectionnez **Administration > Download/Backup Configuration File**.

ÉTAPE 2 Cliquez sur **Show Advanced Settings**.

ÉTAPE 3 Dans la case, saisissez la valeur de départ utilisée pour générer la clé.

ÉTAPE 4 Cliquez sur **Save**.

Mise à niveau du microprogramme

Vous pouvez mettre à niveau le microprogramme vers une version plus récente pour le routeur sur la page **Administration > Firmware Upgrade**.

AVERTISSEMENT Lors d'une mise à niveau du microprogramme, n'essayez pas de naviguer en ligne, ne désactivez pas l'appareil, n'arrêtez pas l'ordinateur et n'interrompez surtout pas le processus jusqu'au terme de l'opération. Ce processus prend environ une minute, redémarrage inclus. L'interruption du processus de mise à niveau à certains moments de l'écriture de la mémoire flash peut l'endommager et rendre le routeur inutilisable.

Mise à niveau du microprogramme

Pour mettre à niveau le microprogramme du routeur vers une version plus récente :

ÉTAPE 1 Sélectionnez **Administration** > **Firmware Upgrade**.

ÉTAPE 2 Dans la section **Firmware Upgrade**, cliquez sur **Download** pour télécharger la dernière version du microprogramme.

ÉTAPE 3 Vous pouvez également mettre le microprogramme à niveau en cliquant sur **Browse** pour localiser et télécharger les derniers fichiers de microprogramme depuis un emplacement précis :

ÉTAPE 4 (Facultatif) Pour rétablir les paramètres par défaut de l'appareil après une mise à niveau du microprogramme, cochez la case **Reset all configurations/settings to factory defaults**.

AVERTISSEMENT Si vous rétablissez les paramètres par défaut du routeur, tous les paramètres de configuration seront supprimés.

ÉTAPE 5 Cliquez sur **Start Upgrade**.

Une fois validée, la nouvelle image du microprogramme est enregistrée dans la mémoire flash et le routeur est automatiquement redémarré avec le nouveau microprogramme.

Étapes de récupération du microprogramme

Si le microprogramme est endommagé pendant la mise à niveau ou une panne de courant, le témoin DEL PWR s'allume en rouge. Pour télécharger et récupérer le microprogramme, procédez comme suit :

ÉTAPE 1 Mettez le routeur hors tension.

ÉTAPE 2 Vous pouvez accéder au mode de récupération du microprogramme de 2 manières différentes. Vous pouvez sélectionner l'une de ces méthodes pour accéder au mode de récupération.

- Si le microprogramme est endommagé et s'il ne peut pas démarrer normalement, le système passe automatiquement en mode de récupération une fois le routeur sous tension. La DEL PWR s'allume en rouge. Généralement, la configuration d'origine est rétablie une fois le nouveau microprogramme téléchargé.
- Pour accéder au mode de récupération manuellement, branchez les câbles de la console (débit en bauds de 115 200). Mettez le système sous tension. Le journal de démarrage s'affiche alors sur le terminal de la console. Appuyez sur une touche quelconque pour interrompre le démarrage normal. La DEL PWR s'allume en rouge. Généralement, la configuration d'origine est rétablie une fois le nouveau microprogramme téléchargé.
- Pour supprimer les configurations d'origine, appuyez sur le bouton de réinitialisation et mettez le routeur sous tension.

ÉTAPE 3 Connectez l'ordinateur au port LAN1. Configurez l'adresse statique de l'ordinateur à 192.168.1.100.

ÉTAPE 4 Récupérez le microprogramme du routeur via l'interface utilisateur Web. Par exemple, vous pouvez saisir « http://192.168.1.1 » dans le navigateur. Choisissez ensuite l'image, par exemple (pour RV132W)
« RV132W_FW_ANNEX_A_1.0.0.10.bin » ou (pour RV134W)
« RV134W_FW_ANNEX_A_1.0.0.10.bin » et appuyez sur Recover & Reboot. Patientez quelques minutes jusqu'à ce que le routeur redémarre et clignote une fois le téléchargement terminé.

ÉTAPE 5 Après le démarrage normal du routeur, la DEL PWR s'allume en vert.

Redémarrage

Pour redémarrer le routeur :

ÉTAPE 1 Sélectionnez **Administration** > **Reboot**.

ÉTAPE 2 Cochez la case **Reboot the device**.

ÉTAPE 3 Cliquez sur **Reboot.**

Restauration des paramètres d'usine

AVERTISSEMENT Lors d'une restauration, n'essayez pas de naviguer en ligne, ne désactivez pas le routeur, n'arrêtez pas l'ordinateur et n'utilisez pas le routeur jusqu'au terme de l'opération. Celle-ci devrait prendre environ une minute. Lorsque le voyant de test s'éteint, patientez encore quelques secondes avant d'utiliser le routeur.

Pour rétablir les paramètres d'usine du routeur :

ÉTAPE 1 Sélectionnez **Administration** > **Reboot**.

ÉTAPE 2 Cochez la case **Return to factory default settings after reboot.**

ÉTAPE 3 Cliquez sur **Reboot**.

9

Problèmes et solutions

Assistance	
Communauté d'assistance Cisco	www.cisco.com/go/smallbizsupport
Assistance et ressources Cisco	www.cisco.com/go/smallbizhelp
Coordonnées de l'assistance téléphonique	www.cisco.com/en/US/support/tsd_cisco_small_business_support_ center_contacts.html
Téléchargements de microprogrammes Cisco	www.cisco.com/go/smallbizfirmware Sélectionnez un lien pour télécharger le microprogramme d'un produit Cisco. Aucune connexion n'est requise.
Demandes Open Source Cisco	Pour recevoir une copie du code source auquel vous avez droit dans le cadre de la ou des licences gratuites ou open source (telles que la Licence publique générale/amoindrie GNU), veuillez envoyer votre demande à l'adresse suivante : external-opensource-requests@cisco.com N'oubliez pas de préciser le nom de votre produit Cisco, sa version, ainsi que son numéro de référence à 18 chiffres (par exemple : 7XEEX17D99-3X49X08 1) que vous trouverez dans la documentation Open Source du produit.
Cisco Partner Central (connexion partenaire requise)	www.cisco.com/web/partners/sell/smb
Routeur VPN multifonction sans fil Cisco RV132W/RV134W	www.cisco.com/en/US/products/ps9923/tsd_products_support_series_home.html