

Configurez les configurations BLÊMES de PPPoE sur le routeur RV34x

Objectif

Ce but de l'article de t'afficher comment configurer les configurations BLÊMES de PPPoE sur le routeur RV34x.

Introduction

Un réseau étendu (WAN) est un réseau qui couvre une zone large. Un utilisateur ou un réseau des utilisateurs peut se connecter à l'Internet par un fournisseur de services Internet (ISP) qui offre de diverses méthodes pour installer un client avec une connexion Internet. Ces méthodes peuvent être le protocole DHCP automatique (DHCP), le Procotole IP (Internet Protocol) statique, le Protocole PPPoE (PPP sur Ethernet), le Protocole PPTP (Point-to-Point Tunneling Protocol), le Layer 2 Tunneling Protocol (L2TP), la passerelle, et la configuration automatique sans état d'adresse (SLAAC) pour l'IPv6.

Configurer les bonnes configurations BLÊMES sur le routeur est nécessaire afin d'installer correctement la connexion Internet basée sur vos spécifications du réseau et installation. Quelques configurations BLÊMES à utiliser sur votre routeur tel que des noms d'utilisateur, des mots de passe, des adresses IP, et des serveurs DNS devraient t'être fournies par votre ISP.

Dans ce scénario, l'installation de l'ISP exige du routeur d'employer des configurations de PPPoE pour se connecter à l'Internet. C'est un protocole réseau qui crée un tunnel virtuel de point final au point final. Le PPPoE exige des qualifications de procédure de connexion de créer la connexion entre l'utilisateur et l'ISP. Ceci fournit la Sécurité supplémentaire puisque l'utilisateur nécessairement n'est pas toujours connecté à l'Internet. Le PPPoE est utilisé principalement avec des services de la ligne d'abonné numérique (DSL) où les utilisateurs se connectent à un modem DSL au-dessus des Ethernets.

Périphériques applicables | Version de logiciel

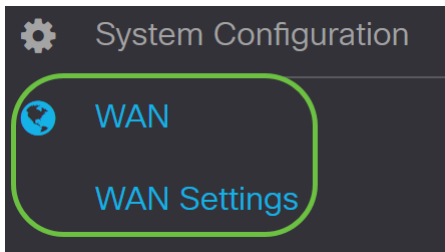
- RV340 | 1.0.01.17 ([téléchargement le plus tard](#))
- RV340W | 1.0.01.17 ([téléchargement le plus tard](#))
- RV345 | 1.0.01.17 ([téléchargement le plus tard](#))
- RV345P | 1.0.01.17 ([téléchargement le plus tard](#))

Configurez les configurations de WAN de PPPoE

L'ISP fournit les paramètres de PPPoE.

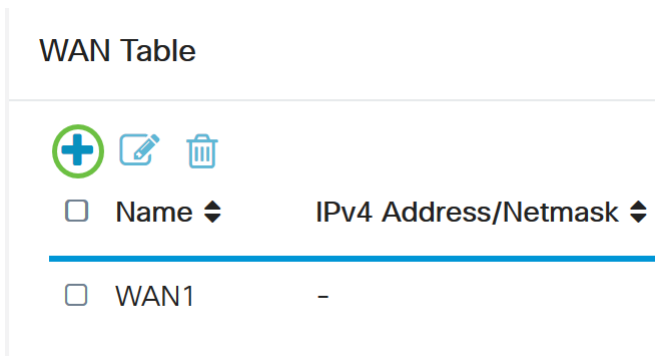
[Étape 1](#)

Accédez à l'utilitaire basé sur le WEB de routeur et choisissez le **WAN > les configurations BLÊMES**.



Étape 2

Dans le *Tableau BLÊME*, cliquez sur le bouton d'ajouter.



Étape 3

Dans la fenêtre *BLÊME de sous-interface d'Add/Edit* qui apparaît, cliquez sur en fonction la sous-interface BLÊME que vous voulez configurer.

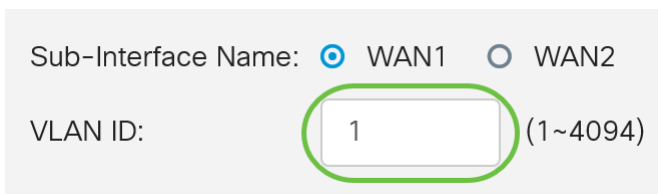
Add/Edit WAN Sub-interface



Dans cet exemple, **WAN1** est choisi. C'est la valeur par défaut.

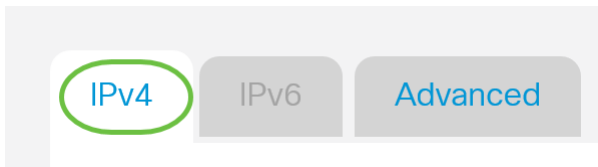
Étape 4

Écrivez l'*ID DE VLAN* dans le champ approprié. Dans cet exemple, **1** est utilisé.



Étape 5

Cliquez sur l'onglet de la connexion que vous utilisez.



Dans cet exemple, l'**ipv4** est choisi. C'est la valeur par défaut. Si vous utilisez l'*IPv6*, ignorez à l'[IPv6](#).

IPv4

Étape 6

Cliquez sur en fonction la case d'option de **PPPoE** pour choisir le *type de connexion*.

- Connection Type:
- DHCP
 - Static IP
 - PPPoE
 - PPTP
 - L2TP
 - Bridge

Étape 7

Sous des *configurations de PPPoE*, écrivez le *nom d'utilisateur* dans le champ approprié.

- Connection Type:
- DHCP
 - Static IP
 - PPPoE
 - PPTP
 - L2TP
 - Bridge

PPPoE Settings

Username:

UserA

Dans cet exemple, **UserA** est utilisé.

Étape 8

Entrez le *mot de passe* dans le champ approprié.

PPPoE Settings

Username:

UserA

Password:

●●●●●●●●

Étape 9

Choisissez le *serveur DNS* du menu déroulant. Les options sont :

- *Serveur DNS fourni par PPPoE d'utilisation* - Permet au routeur pour utiliser le serveur DNS fourni par la connexion PPPoE.
- *DN d'utilisation en tant que ci-dessous* - Permet au routeur pour utiliser les adresses de serveur de DNS que vous spécifierez dans les domaines au-dessous de elle.

DNS Server:

Static DNS 1:

Dans cet exemple, le **PPPoE d'utilisation** a fourni le **serveur DNS** est choisi. C'est la valeur par défaut.

Étape 10

Cliquez sur en fonction une case d'option pour choisir le mode de connecter. Les options sont :

- *Connectez le à la demande* - Permet la connexion Internet seulement quand il y a du trafic. Cette option est idéale si les frais ISP basés sur combien de temps la connexion est en activité. Si vous choisissez cette option, un temps d'inactivité maximum devrait être spécifié. Ceci déterminerait la durée que la connexion peut être de veille avant qu'elle soit terminée.
- *Keepalive* - Cette option permet à la connexion Internet pour être en activité à tout moment.

Connection on Demand.

Max Idle Time min. (Range: 1-9999, Default: 5)

Keep Alive.

Dans cet exemple, la **keepalive** est choisie. C'est la valeur par défaut.

Étape 11

Choisissez le type d'authentification du menu déroulant de *type d'authentification*. Les options sont :

- *Négociation automatique* - Cette option permet au routeur pour envoyer des requêtes au serveur ISP pour déterminer quelle méthode d'authentification doit être utilisée. Le routeur envoie alors les qualifications d'authentification avec le type correct d'authentification.
- *PAP* - Protocole d'identification de mot de passe est un protocole d'authentification qui transmet des mots de passe décryptés ASCII au-dessus du réseau. C'est une méthode d'authentification unsecure.
- *CHAP* - L'authentification Protocol à échanges confirmés est un protocole d'authentification qui vérifie l'authentification par l'utilisation d'une connexion en trois étapes. Cette prise de contact a lieu au moment de la connexion initiale et au hasard des intervalles après la connexion initiale.
- *MS-CHAP* - C'est la version de Microsoft du CHAP. MS-CHAP est dans un format conçu pour la compatibilité avec des Produits de Windows NT.

- **MS-CHAPv2** - C'est une extension de MS-CHAP. MS-CHAPv2 est une méthode d'authentification plus forte que MS-CHAP dû à une clé de chiffrement plus fort.

Authentication Type:

Service Name:

Note: 1. Add this sub-interface to Multi-WAN table to forward the default route traffic based on routing table.

Dans cet exemple, la **négociation automatique** est choisie. C'est la valeur par défaut.

Étape 12

Dans le domaine de *nom de service*, écrivez le nom que l'ISP l'utilise pour définir le type d'accès pour le routeur.

Authentication Type:

Service Name:

Dans cet exemple, **RouterService** est utilisé.

Étape 13

Cliquez sur **Apply**.

Keep Alive.

Authentication Type:

Service Name:

Note: 1. Add this sub-interface to Multi-WAN table to forward the default route traffic. Or it will only forward the connected route traffic based on routing table.

2. This interface Network Service Detection will turn off automatically when protocol is PPPoE. Please go to [Multi-WAN](#) to configure it.

Apply

Cancel

IPv6

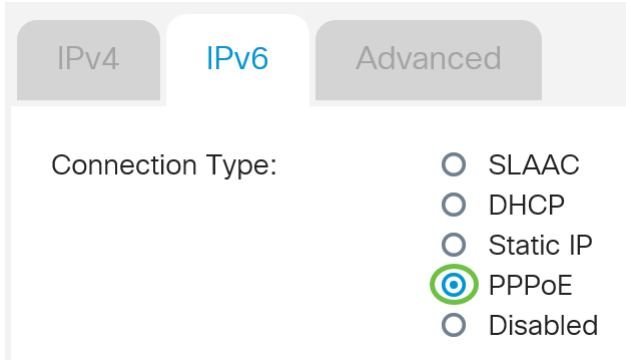
Étape 1

Cliquez sur l'onglet d'**IPv6**.



Étape 2

Cliquez sur en fonction la case d'option de **PPPoE** pour choisir le *type de connexion*.



Étape 3

Dans le *PPPoE les configurations* sectionnent, choisissent un de ce qui suit :

- *Partagez la même session avec l'ipv4* - Sélectionnez le *partage la même session avec l'ipv4* pour réutiliser le même nom d'utilisateur/mot de passe configuré dans la configuration de PPPoE d'ipv4, et obtenez les adresses d'ipv4 et d'IPv6 de la même session de PPPoE.
- *Sessions distinctes d'ipv4 et d'IPv6* - Sélectionnez les *sessions distinctes d'ipv4 et d'IPv6* pour un établissement de nom d'utilisateur/mot de passe qui sera utilisé seulement pour une session de PPPoE d'IPv6.

PPPoE Settings

- Share same session with IPv4 Separate IPv4 and IPv6 sessions

Dans cet exemple, des **sessions distinctes d'ipv4 et d'IPv6** est choisies.

Étape 4

Sous des *configurations de PPPoE*, écrivez le *nom d'utilisateur* dans le champ approprié.

PPPoE Settings

- Share same session with IPv4 Separate IPv4 and IPv6 sessions

Username:

Dans cet exemple, **UserV6** est utilisé.

Étape 5

Entrez le *mot de passe* dans le champ approprié.

PPPoE Settings

Share same session with IPv4 Separate IPv4 and IPv6 sessions

Username:

UserV6

Password:

●●●●●●●●

Étape 6

Cliquez sur la flèche déroulante de *serveur DNS* et choisissez le *serveur DNS*. Les options sont :

- *Serveur DNS fourni par PPPoE d'utilisation* - Permet au routeur pour utiliser les configurations de serveur DNS fournies par la connexion PPPoE.
- *DN d'utilisation en tant que ci-dessous* - Permet au routeur pour utiliser les adresses de serveur de DNS que vous spécifierez dans les domaines au-dessous de elle.

DNS Server:

Use DNS as Below

Static DNS 1:

Use PPPoE Provided DNS Server

Use DNS as Below

Dans cet exemple, **DN d'utilisation comme ci-dessous** est choisi. C'est la valeur par défaut.

Étape 7

Dans les *DN statiques 1* champ, introduisent la première adresse de serveur de DNS fournie à vous par votre ISP.

DNS Server:

Use DNS as Below

Static DNS 1:

2001:4860:4860::8888

Static DNS 2:

Dans cet exemple, **2001:4860:4860::8888** est utilisé.

Étape 8

(Facultatif) dans les *DN statiques 2* mettez en place, introduisez la deuxième adresse de serveur de DNS fournie à vous par votre ISP.

DNS Server:

Static DNS 1:

Static DNS 2:

Dans cet exemple, **2001:4860:4860::8844** est utilisé.

Étape 9

Cliquez sur en fonction une case d'option pour choisir le mode de connecter.

- *Connectez le à la demande* - Permet la connexion Internet seulement quand il y a du trafic. Cette option est idéale si les frais ISP basés sur combien de temps la connexion est en activité. Si vous choisissez cette option, un temps d'inactivité maximum devrait être spécifié. Ceci déterminerait la durée que la connexion peut être de veille avant qu'elle soit terminée.
- *Keepalive* - Cette option permet à la connexion Internet pour être en activité à tout moment.

Connection on Demand.

Max Idle Time min. (Range: 1-9999, Default: 5)

Keep Alive.

Dans cet exemple, la **keepalive** est choisie. C'est la valeur par défaut.

Étape 10

Choisissez le type d'authentification du menu déroulant de *type d'authentification*. Les options sont :

- *Négociation automatique* - Cette option permet au routeur pour envoyer des requêtes au serveur ISP pour déterminer quelle méthode d'authentification doit être utilisée. Le routeur envoie alors les qualifications d'authentification avec le type correct d'authentification.
- *PAP* - Protocole d'identification de mot de passe est un protocole d'authentification qui transmet des mots de passe décryptés ASCII au-dessus du réseau. C'est une méthode d'authentification unsecure.
- *CHAP* - L'authentification Protocol à échanges confirmés est un protocole d'authentification qui vérifie l'authentification par l'utilisation d'une connexion en trois étapes. Cette prise de contact a lieu au moment de la connexion initiale et au hasard des intervalles après la connexion initiale.
- *MS-CHAP* - C'est la version de Microsoft du CHAP. MS-CHAP est dans un format conçu pour la compatibilité avec des Produits de Windows NT.
- *MS-CHAPv2* - C'est une extension de MS-CHAP. MS-CHAPv2 est une méthode d'authentification plus forte que MS-CHAP dû à une clé de chiffrement plus fort.

Authentication Type:

Service Name:

DHCP-PD

Note: 1. Add this sub-interface to Multi-WAN table to forward the default route

Dans cet exemple, la **négoiation automatique** est choisie. C'est la valeur par défaut.

Étape 11

Dans le domaine de *nom de service*, écrivez le nom que l'ISP l'utilise pour définir le type d'accès pour le routeur.

Authentication Type:

Service Name:

Dans cet exemple, **RouterV6** est utilisé.

Étape 12

(Facultatif) vérifiez la case à cocher **DHCP-PD** si vous utilisez la délégation du préfixe DHCPv6.

DHCP-PD Prefix Name:

Étape 13

(Facultatif) écrivez le *nom de préfixe* dans le champ approprié.

DHCP-PD Prefix Name:

Dans cet exemple, **DHCPv6** est utilisé.

Étape 14

Cliquez sur **Apply**.

Authentication Type:

Service Name:

DHCP-PD Prefix Name:

Note: 1. Add this sub-interface to Multi-WAN table to forward the default route traffic. Or it will only forward the connected route traffic based on routing table.

Vous avez maintenant avec succès placé vos configurations de réseau étendu du routeur RV34x au PPPoE.

Visualisez un vidéo lié à cet article...

[A cliquez ici pour visualiser d'autres entretiens de tech de Cisco](#)