

Configuration de la terminaison PPPoE sur un CMTS uBR7100 avec tunnellation L2TP

Contenu

[Introduction](#)

[Avant de commencer](#)

[Conventions](#)

[Conditions préalables](#)

[Composants utilisés](#)

[Théorie générale](#)

[Configurez](#)

[Diagramme du réseau](#)

[Configurations](#)

[Vérifiez](#)

[Procédures](#)

[Dépannez](#)

[Procédure de dépannage](#)

[Dépannage des commandes](#)

[Forum aux questions](#)

[Informations connexes](#)

[Introduction](#)

Ce document fournit une configuration d'échantillon d'arrêt de Protocole PPPoE (PPP sur Ethernet) dans un réseau de Câble haut débit utilisant le système de terminaison par modem câble d'uBR7100 de Cisco (CMTS) comme concentrateur d'accès local (LAC). Dans ce document, la session de PPPoE est initiée par un routeur de Cisco 1600 en tant que PPPoE Client, et transmet le trafic PPP par une connexion en tunnel sécurisée de protocole (L2TP) de perçage d'un tunnel de la couche deux au serveur de réseau L2TP (LNS). Le routeur LNS termine le tunnel L2TP de Cisco CMTS, et peut expédier le trafic au réseau d'entreprise.

[Avant de commencer](#)

[Conventions](#)

Pour plus d'informations sur les conventions de documents, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

[Conditions préalables](#)

Le lecteur de ce document devrait être au courant de [RFC 2516](#) , qui décrit les règles régissant le PPPoE, aussi bien que du protocole de Data-over-Cable Service Interface Specifications (DOCSIS). [Ce document ne décrit pas comment installer le réseau de Câble haut débit physique. Avant de tenter pour configurer une solution de PPPoE, les Modems câble conformes DOCSIS doivent être en ligne et fonctionnants](#) en jetant un pont sur le mode. Pour plus d'informations sur dépanner le CMS, référez-vous aux [Modems câble d'ubr de dépannage n'étant pas livré en ligne](#).

Composants utilisés

Les informations dans ce document sont basées sur les versions de logiciel et de matériel ci-dessous.

- La caractéristique d'arrêt de PPPoE est prise en charge seulement sur la gamme Cisco uBR7100 et les routeurs haut débit universels de Cisco uBR7246VXR (ubr).
- Le routeur de Cisco CMTS doit être la release courante 12.2(4)BC1a de Cisco IOS® ou la version ultérieure. En outre, pour prendre en charge la caractéristique d'arrêt de PPPoE, le nom d'image logicielle doit inclure l'ensemble de caractéristiques IP+ (les lettres « moi » et « s » devons apparaître dans le nom d'image logicielle).
- Pour prendre en charge l'arrêt de PPPoE sur les interfaces de câble empaquetées, le routeur de Cisco CMTS doit être Cisco IOS version 12.2(8)BC2 courante ou une version ultérieure.
- Le logiciel client doit prendre en charge le protocole d'arrêt de PPPoE. Si le système d'exploitation de l'ordinateur n'inclut pas un tel support, l'utilisateur peut utiliser le logiciel client tel que WinPoet. Ce document utilise Cisco 1600 en tant que PPPoE Client.

Les informations dans cette installation particulière de laboratoire sont basées sur le logiciel et les versions de matériel ci-dessous.

- Cisco uBR7111 CMTS exécute la release uBR7100-ik8s-mz.122-11.BC1 de Cisco IOS.
- Le routeur de Cisco 1600 exécute la release Cisco 1600-sy-mz.122-11.T8 de Cisco IOS.

Les informations présentées dans ce document ont été créées à partir de périphériques dans un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si vous travaillez dans un réseau opérationnel, assurez-vous de bien comprendre l'impact potentiel de toute commande avant de l'utiliser.

Théorie générale

Le PPPoE fournit la capacité de connecter un réseau des hôtes au-dessus d'un périphérique d'accès par pontage simple à un concentrateur d'Accès à distance. Le PPPoE peut permettre la liaison directe aux interfaces de câble. Le support du PPPoE sur des interfaces de câble des Routeurs de gammes Cisco uBR7100 et uBR7200 permet au matériel de sites du client (CPE) derrière le modem câblé pour employer le PPP comme mécanisme pour obtenir leurs IP address et pour les utiliser pour tout le trafic de données ultérieur, semblable à un client commuté de PPP. En session commutée de PPP, la session de PPPoE est authentifiée et l'adresse IP est négociée entre le PPPoE Client et le serveur, qui pourraient être un routeur de Cisco CMTS ou une passerelle domestique. Avec ce modèle, chaque hôte utilise sa propre pile de PPP. Par conséquent, le contrôle d'accès, la facturation, et le type de service peuvent être faits sur une base par utilisateur, plutôt qu'une base de par-site. Les fournisseurs de services peuvent prendre en charge les hôtes basés sur de PPPoE Client et de protocole DHCP (DHCP) derrière le même cm.

Le PPPoE a deux étapes distinctes, une étape de détection et une étape de session PPP. Quand un hôte souhaite initier une session de PPPoE, il doit d'abord exécuter la détection pour identifier l'adresse MAC Ethernet du pair et pour établir un PPPoE SESSION_ID. Tandis que le PPP définit des relations peer-to-peer, la détection est en soi des relations de client-serveur. Dans le processus de découverte, un hôte (le client) découvre un concentrateur d'accès (le serveur). Basé sur la topologie du réseau, il peut y avoir plus d'un concentrateur d'accès avec lequel l'hôte peut communiquer. L'étape de détection permet à l'hôte pour découvrir tous les concentrateurs d'accès et puis pour sélectionner un. Quand la détection se termine avec succès, l'hôte et le concentrateur d'accès sélectionné ont les informations qu'ils les utiliseront pour établir leur connexion point-à-point au-dessus des Ethernets. Une fois que la session de PPPoE commence, des données de PPP sont envoyées comme dans n'importe quelle autre encapsulation PPP.

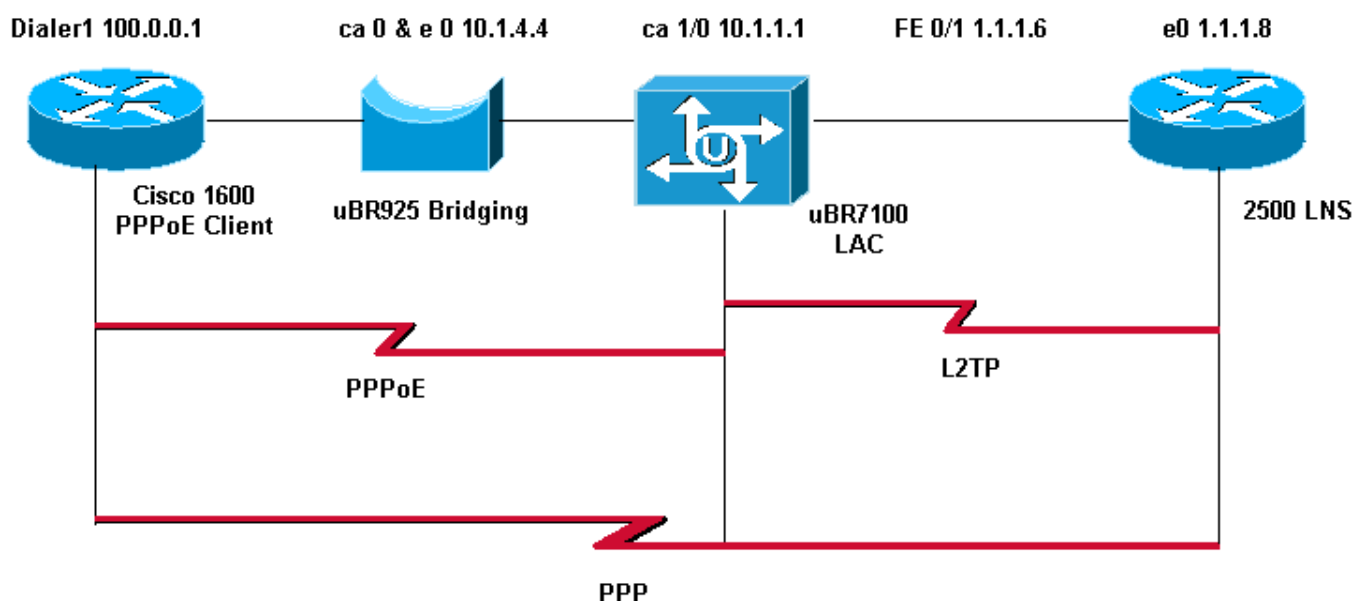
Configurez

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque: Pour obtenir des informations supplémentaires sur les commandes utilisées dans ce document, utilisez l'[Outil de recherche de commande](#) (clients enregistrés seulement).

Diagramme du réseau

Ce document utilise la configuration réseau indiquée dans le diagramme suivant :



Configurations

Ce document utilise les configurations présentées ci-dessous.

Routeur de Cisco 1600 (PPPoE Client)

```
PPPoE_client#show running-config Building
configuration... Current configuration : 1099 bytes !
version 12.2 service timestamps debug uptime service
timestamps log uptime no service password-encryption !
hostname PPPoE_client ! no logging console enable
```

```

password cisco ! username LAC password 0 cisco !---
Cmts-user name/password sent to LNS to create the L2TP
tunnel. username LNS password 0 cisco !--- Lns-user
name/password used by LNS to authenticate tunnel
creation. username user@surf.org !--- Specifies a
username and password for each user to be granted PPPoE
access. !--- This can be configured on the RADIUS
authentication servers. ip subnet-zero no ip domain
lookup ip domain name surf.org ! vpdn enable ! vpdn-
group 1 request-dialin protocol pppoe ! ! ! interface
Ethernet0 no ip address pppoe enable pppoe-client dial-
pool-number 1 ! interface Virtual-Template1 no ip
address ip mtu 1492 no peer default ip address !
interface Serial0 no ip address shutdown no fair-queue !
interface Serial1 no ip address shutdown ! interface
Dialer1 mtu 1492 ip address negotiated ip nat outside
encapsulation ppp dialer pool 1 ppp chap hostname
user@surf.org ppp chap password 0 cisco ! ip nat inside
source list 1 interface Dialer1 overload ip classless ip
route 0.0.0.0 0.0.0.0 Dialer1 no ip http server ! !
access-list 1 permit any ! ! line con 0 line vty 0 4
password cisco login ! end

```

UBR7100 CMTS (LAC) de Cisco

```

LAC#show running-config Building configuration...
Current configuration : 2442 bytes ! version 12.2
service timestamps debug datetime msec service
timestamps log datetime msec no service password-
encryption ! hostname "LAC" ! no logging console enable
password cisco ! !--- Cmts-user name/password sent to
LNS to create the L2TP tunnel. username LAC password 0
cisco !--- Lns-user name/password used by LNS to
authenticate tunnel creation. username LNS password 0
cisco !--- Specifies a username and password for each
user to be granted PPPoE access. !--- This can be
configured on the RADIUS authentication servers.
username user@surf.org no cable qos permission create no
cable qos permission update cable qos permission modems
cable time-server ! cable config-file platinum.cm
service-class 1 max-upstream 128 service-class 1
guaranteed-upstream 10 service-class 1 max-downstream
10000 service-class 1 max-burst 1600 cpe max 10
timestamp ! ip subnet-zero ! ! no ip domain lookup ! ip
dhcp pool pppoe network 10.1.4.0 255.255.255.0 bootfile
platinum.cm next-server 10.1.4.1 default-router 10.1.4.1
option 7 ip 10.1.4.1 option 4 ip 10.1.4.1 option 2 hex
ffff.8f80 lease 7 0 10 ! ip dhcp pool pppoe_clients
network 172.16.29.0 255.255.255.224 next-server
172.16.29.1 default-router 172.16.29.1 domain-name
surf.org lease 7 0 10 ! !--- Enables Virtual Private
Dial-Up Networking (VPDN). vpdn enable vpdn logging !---
VPDN group 1 configures the router to accept PPPoE
connections. !--- Specifies the virtual template used
for the virtual interfaces that are created !--- for
each PPPoE session. ! vpdn-group 1 accept-dialin
protocol pppoe virtual-template 1 !--- VPDN group 2
configures the group to be used for the L2TP tunnel to
the LNS. !--- PPPoE sessions will be initiated from
clients using the domain surf.org. vpdn-group 2 request-
dialin protocol l2tp domain surf.org initiate-to ip
1.1.1.8 local name LAC !--- Disables authentication for
creation of L2TP tunnel. no l2tp tunnel authentication !
! ! ! interface FastEthernet0/0 ip address 2.2.2.2
255.255.255.0 duplex auto speed auto ! interface

```

```

FastEthernet0/1 ip address 1.1.1.6 255.255.255.0 ip
broadcast-address 1.1.1.255 no ip route-cache no ip
mroute-cache duplex auto speed 10 ! interface Cable1/0
ip address 172.16.29.1 255.255.255.224 secondary ip
address 10.1.4.1 255.255.255.0 cable downstream annex B
cable downstream modulation 64qam cable downstream
interleave-depth 32 cable downstream frequency 471000000
cable downstream channel-id 0 no cable downstream rf-
shutdown cable downstream rf-power 51 cable upstream 0
frequency 32000000 cable upstream 0 power-level 0 no
cable upstream 0 shutdown cable dhcp-giaddr policy !---
pppoe enable must be configured on the cable !---
interface accepting PPPoE sessions. !--- This is not
necessary on subinterfaces. pppoe enable ! interface
Virtual-Templat1 ip unnumbered FastEthernet0/1 ip mtu
1492 ppp authentication chap ! ip classless no ip http
server ! ! cdp run ! snmp-server community private RW
snmp-server enable traps tty alias exec scm show cable
modem ! line con 0 line aux 0 line vty 0 4 password
cisco login line vty 5 15 login ! end

```

Cisco 2500 (LNS)

```

hostname "LNS" ! ! !--- Lns-user name/password for the
LNS itself. username LNS password 0 cisco !--- Cmts-user
name/password for the Cisco CMTS. username LAC password
0 cisco !--- Username and password for the PPPoE client.
!--- This can be configured on the RADIUS authentication
servers. username user@surf.org password 0 cisco ! vpdn
enable ! !--- Creates a VPDN group and starts VPDN group
configuration mode. vpdn-group 1 accept-dialin !---
Configures VPDN group for L2TP protocol so that it !---
can access the PPPoE server. protocol l2tp !---
Specifies the virtual-template number to be used when !-
-- configuring a PPPoE session. virtual-template 1 !---
This group terminates L2TP tunnels from the specified
CMTS hostname. terminate-from hostname LAC !--- This is
the local hostname of the LNS. local name LNS !---
Disables authentication for creation of L2TP tunnel. no
l2tp tunnel authentication ! ! ! interface Virtual-
Templat1 ip unnumbered FastEthernet0/1 ip mtu 1492 !---
Surf is used as the pool name, and !--- the router will
use an address from the 100-net. !--- If a test cannot
be found, it will search for the pool with the name
default. peer default ip address pool surf ppp
authentication chap ! ip local pool surf 100.0.0.1
100.0.0.10

```

Vérfiez

Cette section présente des informations que vous pouvez utiliser pour vous assurer que votre configuration fonctionne correctement.

Certaines commandes **show** sont prises en charge par l'[Output Interpreter Tool](#) ([clients enregistrés](#) uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

Procédures

Pour vérifier qu'une adresse IP est distribuée du groupe LNS, suivez les étapes ci-dessous.

1. Émettez la commande de **show ip local pool** du LNS. Vérifiez la sortie de commande.

```
LNS#show ip local pool Pool Begin End Free In use surf 100.0.0.1 100.0.0.10 9 1
```
2. Pour identifier l'appelant réussi, émettez la commande d'**IP de show caller** du LNS.

```
LNS#show caller ip Line User IP Address Local Number Remote Number <-> Vi29 user@surf.org 100.0.0.1 - - in
```
3. Pour vérifier la session VPDN sur le LNS, émettez l'ordre de **show vpdn session**.

```
LNS#show vpdn session L2TP Session Information Total tunnels 1 sessions 1 LocID RemID TunID Intf Username State Last Chg Fastswitch 30 299 23629 Vi29 user@surf.org est 00:16:03 enabled %No active L2F tunnels %No active PPTP tunnels %No active PPPoE tunnels
```

Employez les étapes ci-dessous pour vérifier le nombre d'interface de modèle virtuel qui est utilisé par un PPPoE Client.

1. Émettez l'ordre de **show vpdn session** du LAC. Vérifiez la sortie de commande.

```
LAC# show vpdn session L2TP Session Information Total tunnels 1 sessions 1 LocID RemID TunID Intf Username State Last Chg Fastswitch 299 30 26280 Vi1 user@surf.org est 00:31:19 enabled %No active L2F tunnels %No active PPTP tunnels PPPoE Session Information Total tunnels 1 sessions 1 PPPoE Session Information SID RemMAC LocMAC Intf VAST OIntf VLAN/VP/VC 1 0030.9413.0556 0008.a328.831c Vi1 UP Cal/0
```
2. Pour afficher les utilisateurs qui se sont inscrits à Cisco CMTS utilisant le PPPoE, émettez la commande de **modem câblé de show interface cable**.

```
LAC#show interface cable 1/0 modem 0 SID Priv bits Type State IP address method MAC address 1 00 modem up 10.1.4.2 dhcp 0010.9526.2f57 2 00 modem up 10.1.4.3 dhcp 0007.0e03.a7e5 2 00 host unknown 172.16.29.2 static 0007.0e03.a7e4 3 00 modem up 10.1.4.4 dhcp 0007.0e02.c893 3 00 host unknown pppoe 0030.9413.0556 4 00 modem up 10.1.4.5 dhcp 0007.0e03.5075
```
3. Pour afficher les domaines du courant VPDN, émettez la commande de **show vpdn domain**.

```
LAC#show vpdn domain Tunnel VPDN Group ----- domain:surf.org2 (L2TP)
```

Dépannez

Procédure de dépannage

Utilisez les instructions ci-dessous de dépanner votre configuration.

1. Vérifiez le LAC pour voir le statut des interfaces en émettant la **commande brief de show ip interface**. Si les interfaces l'un des sont en baisse, vérifiez le câble physique et assurez-vous que les interfaces ne sont pas administrativement en baisse.

```
LAC#show ip interface brief Interface IP-Address OK? Method Status Protocol FastEthernet0/0 2.2.2.2 YES NVRAM up up FastEthernet0/1 1.1.1.6 YES NVRAM up up Cable1/0 10.1.4.1 YES NVRAM up up Virtual-Access1 1.1.1.6 YES TFTP up up Virtual-Templatel 1.1.1.6 YES unset down down
```
2. Vérifiez l'interface sur le PPPoE_client pour vérifier que l'interface de numérotation est en hausse et a une adresse IP du groupe LNS.

```
PPPoE_client#show ip interface brief Interface IP-Address OK? Method Status Protocol Dialer1 100.0.0.1 YES BOOTP up up Ethernet0 unassigned YES NVRAM up up Serial0 unassigned YES NVRAM up up Serial1 unassigned YES NVRAM up up Virtual-Access1 unassigned YES unset up up
```
3. Assurez-vous que vous pouvez cingler le LNS du PPPoE Client.

```
PPPoE_client#ping 1.1.1.8 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 1.1.1.8, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 12/12/16 ms
```
4. Si vous avez des problèmes initiant L2TP, essayez émettre la commande de **sur-non-concordance de lcp renegotiation** configurée sur le LNS sous le VPDN-groupe.

```
LNS#config t Enter configuration commands, one per line. End with CNTL/Z. LNS(config)#vpdn-group 1 LNS(config-vpdn)#lcp renegotiation on-mismatch
```

Remarque: Le Link Control Protocol de proxys de LAC (LCP) quand débuts de PPP. Quand le LNS commence voyant le PPP expédié, il regarde le LCP et s'il n'est pas ce qui il aurait été en pourparlers avec le client lui-

même, il se plaint. La commande de sur-**non-concordance de lcp renegotiation** force le LNS pour renégocier LCP avec le client. Non tous les clients renégocieront LCP, cependant, la plupart d'entre eux pour faire.

Dépannage des commandes

Certaines commandes **show** sont prises en charge par l'[Output Interpreter Tool \(clients enregistrés\)](#) uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

Remarque: Avant d'exécuter les commandes **debug**, référez-vous à la section **Informations importantes sur les commandes Debug**.

- **debug ppp negotiation** — Émettre cette commande sur le LNS te permet pour visualiser les transactions de négociation PPP pour identifier le problème ou pour le présenter quand l'erreur se produit et élabore une résolution. Il est impératif, cependant, que vous comprenez la sortie de **debug ppp negotiation**. [La compréhension de la sortie de debug ppp negotiation](#) fournit une méthode complète pour lire et dépanner le PPP.
- **erreurs du debug vpdn 12x-packet** — lissuing cette commande affiche L2F et erreurs de protocole L2TP qui empêchent l'établissement ou le fonctionnement normal de tunnel
- **événements du debug vpdn 12x-packet** — Émettre cette commande sur le LNS affiche les événements L2TP qui font partie d'établissement de tunnel ou arrêt.
- **paquet de debug vpdn [contrôle / les données] [détail]** - émettant cette commande sur le LNS ou le LAC affichent les informations d'en-tête de paquet de Protocol-particularité, telles que des numéros de séquence si présent, indicateurs, et longueur.
- **événement de debug vpdn [protocole / flow-control]** — émettre cette commande sur le LNS ou le LAC affiche des erreurs VPN et des événements de base dans les limites du protocole L2TP et des erreurs associés avec le contrôle de flux où le pair distant reçoivent la fenêtre est configurés pour une valeur plus grande que zéro.
- **debug ppp {CHAP / PAP}** — émettre cette commande affiche le protocole d'authentification CHAP (Challenge Handshake Authentication Protocol) et le Password Authentication Protocol (PAP) qui est établie dans le PPP.
- **debug ip udp** — Émettant cette commande sur le LNS vérifie la sortie pour voir si des paquets sont reçus de l'hôte de PPPoE.
- **debug aaa per-user** — Émettant cette commande des affichages LNS quels attributs sont appliqués à chaque utilisateur pendant que l'utilisateur authentifie.
- **debug radius** — Émettant cette affiche des informations de commande associée quand les utilisateurs authentifient utilisant un serveur de RAYON.

Forum aux questions

Q. Cisco CMTS prend en charge-il l'expédition de PPPoE ?

R. Non. Les Routeurs de Cisco CMTS ne prennent en charge pas l'expédition de PPPoE, qui reçoit des paquets de PPPoE d'une interface entrante et en avant eux sur une interface sortante. Les Routeurs de gamme Cisco uBR7100 expédient automatiquement le trafic de PPPoE une fois configurés pour MxU jetant un pont sur le mode (qui est pris en charge seulement sur l'EC de Cisco IOS version 12.1), cependant, c'est une conséquence de la configuration traversière et non dû à n'importe quel Soutien PPPoE. Pour fournir la clarté, l'expédition de PPPoE n'est pris en charge sur aucun Cisco CMTS.

Q. Est-ce que je peux avoir des PPPoE Client et des clients réguliers du protocole DHCP (DHCP) en même temps sur la même usine DOCSIS ?

R. Oui. L'utilisation simultanée de prises en charge de fonctionnalité d'arrêt de PPPoE des PPPoE Client et des clients DHCP derrière le même CMS. Les abonnés peuvent utiliser le PPPoE pour leur login initial au réseau câblé, et puis emploient le DHCP pour permettre à leurs autres PC et à d'autres hôtes pour obtenir des adresses IP pour l'accès au réseau.

Q. Y a-t-il du Soutien PPPoE pour le NPE-300 et NPE-400 sur les Plateformes de Cisco uBR7200VXR CMTS ?

R. Oui. Le processeur NPE-300 a atteint son échéance en août 15 de fin de vie, 2001, cependant.

Q. Le PPPoE est-il pris en charge sur la plate-forme de Cisco uBR10k CMTS ?

R. Non. La caractéristique d'arrêt de PPPoE est seulement prise en charge sur les Routeurs de gamme Cisco uBR7100 et le routeur de Cisco uBR7246VXR, utilisant la Cisco IOS version 12.2(4)BC1a ou ultérieures. Il n'est pas pris en charge sur le routeur de Cisco uBR10012.

Q. Combien de sessions de PPPoE est-ce que je peux exécuter sur la plate-forme de Cisco CMTS ?

R. La plate-forme d'ubr hérite d'une limite BID de 10000 la de la plate-forme de Cisco 7200 qui prend en charge 4000 sessions de PPPoE avec un NPE-225 et un NPE-300 tandis que 8000 sessions de PPPoE sont prises en charge avec un NPE-400. La plate-forme d'uBR7100 qui n'a pas pour avoir NPEs modulaire, prend en charge 4000 sessions de PPPoE. Ce sont des limites théoriques. Vous devez considérer ce le nombre maximal de sessions actives et simultanées de PPPoE est moins, selon la quantité de mémoire à bord de la carte processeur, le type de cartes d'interface de câble étant utilisées, la bande passante consommé par chaque utilisateur, et la configuration du routeur.

Q. Quelle release de Cisco IOS est arrêt de PPPoE l'a pris en charge dans la série EC ?

R. La caractéristique d'arrêt de PPPoE n'est prise en charge sur aucun routeur de Cisco CMTS en utilisant l'EC de Cisco IOS version 12.1.

[Informations connexes](#)

- [Fonction PPPoE Session limit](#)
- [PPP au-dessus des Ethernets](#)
- [PPPoE sur ATM](#)
- [Cisco - Architecture de référence de PPPoE pour Cisco UAC 6400](#)
- [Protocole point-à-point au-dessus d'arrêt d'Ethernets sur Cisco CMTS](#)
- [RFC 2516](#)
- [Support technique - Cisco Systems](#)