

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

Contenu

[Introduction](#)

[Avant de commencer](#)

[Conventions](#)

[Conditions préalables](#)

[Components Used](#)

[Théorie générale](#)

[Configuration](#)

[Diagramme du réseau](#)

[Configurations](#)

[Vérification](#)

[Procédures](#)

[Dépannage](#)

[Procédure de dépannage](#)

[Dépannage des commandes](#)

[Forum aux questions](#)

[Informations connexes](#)

[Introduction](#)

Ce document fournit un exemple de configuration de terminaison PPPoE (Point-to-Point Protocol over Ethernet) dans un réseau câblé à large bande utilisant le système CMTS (Cable Modem Termination System) Cisco uBR7100 comme concentrateur d'accès local (LAC). Dans ce document, la session PPPoE est initiée par un routeur Cisco 1600 en tant que client PPPoE et transmet le trafic PPP via une connexion de tunnel L2TP (Layer Two Tunneling Protocol) sécurisée au serveur de réseau L2TP (LNS). Le routeur LNS termine le tunnel L2TP à partir du CMTS Cisco et peut transférer le trafic vers le réseau d'entreprise.

[Avant de commencer](#)

[Conventions](#)

For more information on document conventions, refer to the [Cisco Technical Tips Conventions](#).

[Conditions préalables](#)

Le lecteur de ce document doit connaître la [RFC 2516](#), qui décrit les règles régissant PPPoE,

ainsi que le protocole DOCSIS (Data-over-Cable Service Interface Specifications). Ce document ne décrit pas comment configurer le réseau câblé à large bande physique. Avant de tenter de configurer une solution PPPoE, les modems câble conformes à DOCSIS doivent être en ligne et fonctionner en mode `pontage`. Pour plus d'informations sur le dépannage de CMS, référez-vous à [Dépannage des modems câble uBR non disponibles en ligne](#).

Components Used

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

- La fonctionnalité de terminaison PPPoE est prise en charge uniquement sur les routeurs à large bande universels Cisco uBR7100 et Cisco uBR7246VXR (uBR).
- Le routeur CMTS Cisco doit exécuter Cisco IOS® version 12.2(4)BC1a ou ultérieure. En outre, pour prendre en charge la fonction de terminaison PPPoE, le nom de l'image logicielle doit inclure le jeu de fonctions IP+ (les lettres « i » et « s » doivent apparaître dans le nom de l'image logicielle).
- Pour prendre en charge la terminaison PPPoE sur les interfaces de câble groupées, le routeur Cisco CMTS doit exécuter Cisco IOS version 12.2(8)BC2 ou une version ultérieure.
- Le logiciel client doit prendre en charge le protocole de terminaison PPPoE. Si le système d'exploitation de l'ordinateur n'inclut pas cette prise en charge, l'utilisateur peut utiliser un logiciel client tel que WinPoet. Ce document utilise un Cisco 1600 comme client PPPoE.

Les informations contenues dans cette configuration de travaux pratiques sont basées sur les versions logicielles et matérielles ci-dessous.

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

Les informations présentées dans ce document ont été créées à partir de périphériques dans un environnement de laboratoire spécifique. All of the devices used in this document started with a cleared (default) configuration. 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 protocole PPPoE permet de connecter un réseau d'hôtes via un simple périphérique d'accès par pontage à un concentrateur d'accès distant. PPPoE permet une connexion directe aux interfaces de câble. La prise en charge de PPPoE sur les interfaces de câble des routeurs des gammes Cisco uBR7100 et uBR7200 permet à l'équipement client (CPE) derrière le modem câble d'utiliser le protocole PPP comme mécanisme pour obtenir leurs adresses IP et l'utiliser pour tout le trafic de données ultérieur, comme un client PPP commuté. Dans une session commutée PPP, la session PPPoE est authentifiée et l'adresse IP est négociée entre le client PPPoE et le serveur, qui peut être un routeur Cisco CMTS ou une passerelle domestique. Avec ce modèle, chaque hôte utilise sa propre pile PPP. Par conséquent, le contrôle d'accès, la facturation et le type de service peuvent être effectués par utilisateur plutôt que par site. Les fournisseurs de services peuvent prendre en charge les clients PPPoE et les hôtes DHCP (Dynamic Host Configuration Protocol) derrière le même CM.

Le protocole PPPoE comporte deux étapes distinctes : une étape de découverte et une étape de session PPP. Lorsqu'un hôte souhaite lancer une session PPPoE, il doit d'abord effectuer une détection pour identifier l'adresse MAC Ethernet de l'homologue et établir un ID de session

PPPoE. Alors que le protocole PPP définit une relation peer-to-peer, la découverte est intrinsèquement une relation client-serveur. Dans le processus de découverte, un hôte (le client) découvre un concentrateur d'accès (le serveur). En fonction de la topologie du réseau, il peut y avoir plusieurs concentrateurs d'accès avec lesquels l'hôte peut communiquer. L'étape de découverte permet à l'hôte de découvrir tous les concentrateurs d'accès, puis d'en sélectionner un. Une fois la détection terminée, l'hôte et le concentrateur d'accès sélectionné disposent des informations qu'ils utiliseront pour établir leur connexion point à point sur Ethernet. Une fois que la session PPPoE commence, les données PPP sont envoyées comme dans toute autre encapsulation PPP.

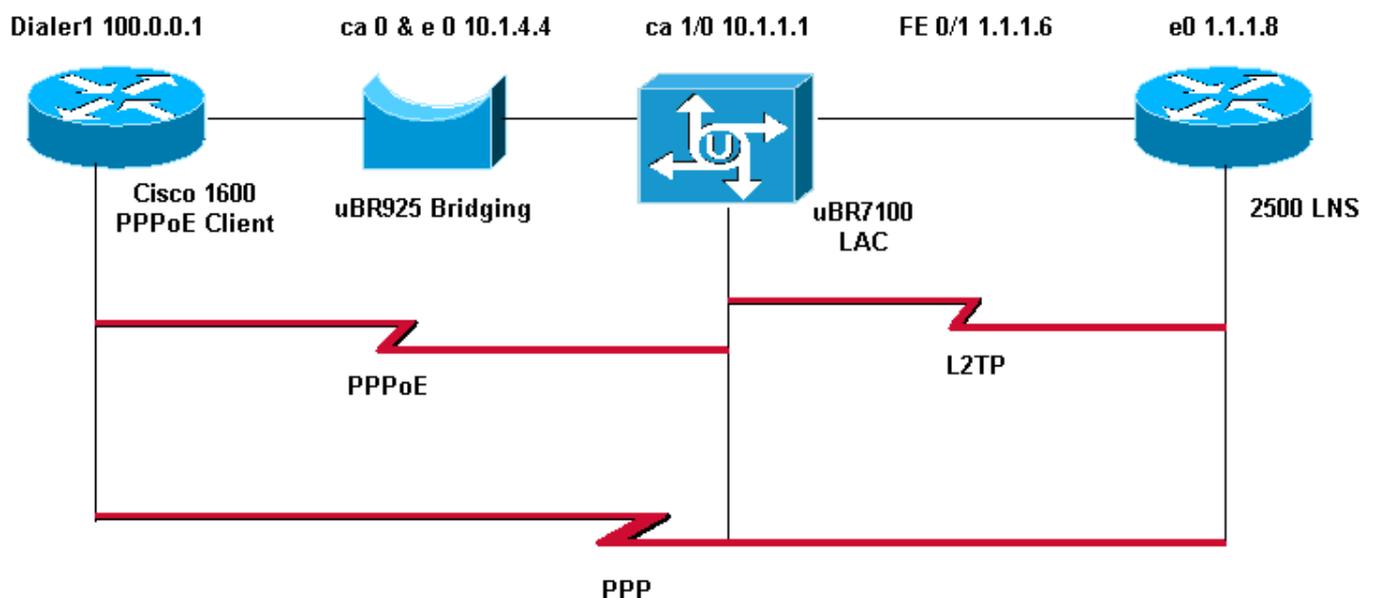
Configuration

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

Remarque : Pour en savoir plus sur les commandes utilisées dans le présent document, utilisez [l'outil de recherche de commandes](#) (clients [inscrits](#) 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 Cisco 1600 (client PPPoE)

```
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
username LNS password 0 cisco

!--- Lns-user name/password used by LNS to authenticate tunnel creation. username user@surf.org
username user@surf.org 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. 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
```

CMTS Cisco uBR7100 (LAC)

```
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
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-Template1
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-Template1
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

```

Vérification

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 à partir du pool LNS, procédez comme suit.

1. Émettez la commande **show ip local pool** à partir du LNS. Vérifiez le résultat de la 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, exécutez la commande **show caller ip** à partir 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, exécutez la commande **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
```

Suivez les étapes ci-dessous pour vérifier le numéro d'interface de modèle virtuel utilisé par un client PPPoE.

1. Émettez la commande **show vpdn session** à partir du LAC. Vérifiez le résultat de la 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	Ca1/0	

2. Pour afficher les utilisateurs qui se sont inscrits au système Cisco CMTS à l'aide de PPPoE, exécutez la commande **show interface cable modem**.

```
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 VPDN actuels, exécutez la commande **show vpdn domain**.

```
LAC#show vpdn domain
```

```
Tunnel VPDN Group
```

```
-----
```

```
domain:surf.org2 (L2TP)
```

[Procédure de dépannage](#)

Suivez les instructions ci-dessous pour dépanner votre configuration.

1. Vérifiez le LAC pour voir l'état des interfaces en exécutant la commande **show ip interface brief**. Si l'une des interfaces est désactivée, vérifiez le câble physique et assurez-vous que les interfaces ne sont pas désactivées administrativement.

```
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-Template1	1.1.1.6	YES	unset	down	down

2. Vérifiez l'interface sur le client PPPoE_client pour vérifier que l'interface de numérotation est active et possède une adresse IP du pool 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 envoyer une requête ping au LNS à partir du client PPPoE.

```
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 rencontrez des problèmes pour lancer L2TP, essayez d'exécuter la commande **lcp renegotiation on-dismatch** configurée sur le LNS sous VPDN-group.

```
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 protocole LCP (Link Control Protocol) proxy LAC au démarrage du protocole PPP. Lorsque le LNS commence à voir le protocole PPP transféré, il examine le protocole LCP et s'il n'est pas ce qu'il aurait négocié avec le client lui-même, il se plaint. La commande **lcp renegotiation on-mismatch** force le LNS à renégocier le LCP avec le client. Tous les clients ne renégocieront pas le protocole LCP, mais la plupart le font.

[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.

Note : Avant d'émettre des commandes **debug**, consultez [Informations importantes sur les commandes de débogage](#).

- **debug ppp negotiation** - L'émission de cette commande sur le LNS vous permet d'afficher les transactions de négociation PPP pour identifier le problème ou l'étape lorsque l'erreur se produit et développer une résolution. Il est toutefois impératif que vous compreniez la sortie **debug ppp negotiation**. [Comprendre la sortie de la négociation debug ppp](#) fournit une méthode complète de lecture et de dépannage de PPP.
- **debug vpdn 12x-packet errors** - L'émission de cette commande affiche les erreurs de protocole L2F et L2TP qui empêchent l'établissement du tunnel ou le fonctionnement normal
- **debug vpdn 12x-packet events** - L'émission de cette commande sur le LNS affiche les événements L2TP qui font partie de l'établissement ou de l'arrêt du tunnel.
- **debug vpdn packet [control / data] [detail]** - l'exécution de cette commande sur le LNS ou le LAC affiche des informations d'en-tête de paquet spécifiques au protocole, telles que les numéros de séquence s'ils sont présents, les indicateurs et la longueur.
- **debug vpdn event [protocol / flow-control]** - L'émission de cette commande sur le LNS ou le LAC affiche les erreurs VPN et les événements de base dans le protocole L2TP et les erreurs associées au contrôle de flux, où la fenêtre de réception de l'homologue distant est configurée pour une valeur supérieure à zéro.
- **debug ppp {chap / pap}** - L'émission de cette commande affiche le protocole CHAP (Challenge Handshake Authentication Protocol) et le protocole PAP (Password Authentication Protocol) intégrés au protocole PPP.
- **debug ip udp** - L'émission de cette commande sur le LNS vérifie le résultat pour voir si des paquets sont reçus de l'hôte pppoe.
- **debug aaa per-user** - L'émission de cette commande à partir du LNS affiche les attributs appliqués à chaque utilisateur lors de l'authentification de l'utilisateur.
- **debug radius** — L'émission de cette commande affiche les informations associées lorsque les utilisateurs s'authentifient à l'aide d'un serveur RADIUS.

[Forum aux questions](#)

Q. Cisco CMTS prend-il en charge le transfert PPPoE ?

A. Non. Les routeurs CMTS Cisco ne prennent pas en charge le transfert PPPoE, qui reçoit les paquets PPPoE d'une interface entrante et les transfère sur une interface sortante. Les routeurs de la gamme Cisco uBR7100 transfèrent automatiquement le trafic PPPoE lorsqu'ils sont configurés pour le mode de pontage MxU (qui est pris en charge uniquement sur Cisco IOS version 12.1 EC). Cependant, ceci est une conséquence de la configuration du pontage et non pas due à la prise en charge de PPPoE. Pour plus de clarté, le transfert PPPoE n'est pris en charge sur aucun système CMTS Cisco.

Q. Puis-je avoir des clients PPPoE et des clients DHCP (Dynamic Host Configuration Protocol) réguliers en même temps sur la même installation DOCSIS ?

A. Oui. La fonction de terminaison PPPoE prend en charge l'utilisation simultanée de clients PPPoE et de clients DHCP derrière les mêmes CM. Les abonnés peuvent utiliser PPPoE pour leur connexion initiale au réseau câblé, puis utiliser DHCP pour permettre à leurs autres PC et autres hôtes d'obtenir des adresses IP pour l'accès au réseau.

Q. Le protocole PPPoE est-il pris en charge pour les plates-formes CMTS NPE-300 et NPE-400

