

Configuración de la finalización de PPPoE en un uBR7100 CMTS con tunelización L2TP

Contenido

[Introducción](#)

[Antes de comenzar](#)

[Convenciones](#)

[prerrequisitos](#)

[Componentes Utilizados](#)

[Teoría Precedente](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Verificación](#)

[Procedimientos](#)

[Troubleshooting](#)

[Procedimiento de Troubleshooting](#)

[Comandos para resolución de problemas](#)

[Preguntas Frecuentes](#)

[Información Relacionada](#)

[Introducción](#)

Este documento proporciona una configuración de muestra de la terminación del Point-to-Point Protocol over Ethernet (PPPoE) en una red de Banda ancha por cable usando el Sistema de terminación del cablemódem (CMTS) del Cisco uBR7100 como el concentrador del Acceso local (LAC). En este documento, a un Cisco 1600 Router inicia como el Cliente de PPPoE, y transmite a la sesión PPPoE el tráfico PPP a través de una conexión del túnel segura del protocolo layer two tunneling (L2TP) al L2TP Network Server (LNS). El router LNS finaliza el túnel L2TP de Cisco CMTS y puede reenviar el tráfico a la red corporativa.

[Antes de comenzar](#)

[Convenciones](#)

Para obtener más información sobre las convenciones del documento, consulte las [Convenciones de Consejos Técnicos de Cisco](#).

[prerrequisitos](#)

[El lector de este documento debe estar familiarizado con el RFC 2516 que describe las reglas que gobiernan el PPPoE y el protocolo de Data-over-Cable Service Interface Specifications \(DOCSIS\). Este documento no describe cómo configurar la red física de cable de banda ancha. Antes de intentar configurar una solución PPPoE, el Cable módems del compatible con DOCSIS debe ser en línea y de funcionamiento en el Bridging Mode. \[Para obtener más información sobre la solución de problemas de CMS, consulte Resolución de problemas de cablemódems uBR que no funcionan.\]\(#\)](#)

Componentes Utilizados

La información que contiene este documento se basa en las versiones de software y hardware indicadas a continuación.

- La función de terminación de PPPoE se admite sólo en los routers de banda ancha universal (uBR) Cisco uBR7100 y Cisco uBR7246VXR.
- El router CMTS de Cisco debe funcionar con la versión 12.2(4)BC1a de Cisco IOS® o la versión posterior. Además, para soportar la característica de la terminación PPPoE, el nombre de la imagen del software debe incluir al conjunto de características IP+ (las cartas “yo” y “s” deben aparecer en el nombre de la imagen del software).
- Para soportar la terminación PPPoE en las interfaces de agrupamiento de cables, el router Cisco CMTS debe estar ejecutando la versión 12.2(8)BC2 del IOS de Cisco o superior.
- El software de cliente debe soportar el protocolo de terminación PPPoE. Si el sistema operativo del ordenador no incluye tal soporte, el usuario puede utilizar el software de cliente tal como WinPoet. Este documento utiliza un Cisco 1600 como el PPPoE cliente.

La información en esta configuración de laboratorio determinada se basa en la siguiente versión de software y hardware.

- El Cisco uBR7111 CMTS es el Cisco IOS Release corriente uBR7100-ik8s-mz.122-11.BC1.
- El Cisco 1600 Router es Cisco IOS Release corriente Cisco 1600-sy-mz.122-11.T8.

La información que se presenta en este documento se originó a partir de dispositivos dentro de un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener un comando antes de ejecutarlo.

Teoría Precedente

PPPoE ofrece la posibilidad de conectar una red de hosts sobre un dispositivo de acceso por puente simple a un concentrador de acceso remoto. PPPoE puede permitir la conexión directa con interfaces de cable. El soporte del PPPoE en las interfaces del cable del Cisco uBR7100 y del Routers de las uBR7200 Series permite que el Customer Premises Equipment (CPE) detrás del módem de cable utilice el PPP como mecanismo para conseguir sus IP Addresses y para utilizarlos para todo el tráfico de datos subsiguientes, similar a un cliente PPP de marcado manual. En una sesión de marcado manual PPP, autentican a la sesión PPPoE y la dirección IP se negocia entre el Cliente de PPPoE y el servidor, que podrían ser un router CMTS de Cisco o un gateway de inicio. Con este modelo, cada host usa su propia pila de PPP. Por lo tanto, el control de acceso, la facturación y el tipo de servicio pueden realizarse en base a cada usuario, en vez de en base a cada sitio. Los proveedores de servicio pueden admitir clientes PPPoE y host basados en Protocolo de configuración de host dinámico (DHCP) detrás del mismo CM.

PPPoE tiene dos etapas distintas, una etapa de detección y una etapa de sesión PPP. Cuando un host desea iniciar a una sesión PPPoE, debe primero realizar la detección para identificar el Ethernet MAC Address del par y para establecer un PPPoE SESSION_ID. Mientras que el PPP define una relación entre peers, la detección es intrínsecamente una relación cliente servidor. Durante el proceso de detección, un host (el cliente) descubre un concentrador de acceso (el servidor). En función de la topología de red, existe más de un concentrador de acceso con el que el host puede comunicarse. La etapa de detección permite que el host detecte a todos los concentradores de acceso y luego seleccione uno. Cuando la detección se completa correctamente, tanto el host como el concentrador de acceso seleccionado poseen la información que usarán para establecer la conexión punto a punto por Ethernet. Una vez que comienza la sesión PPPoE, los datos PPP se envían como en cualquier otra encapsulación PPP.

Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Para obtener información adicional sobre los comandos que se utilizan en este documento, use la Command Lookup Tool (solo para clientes [registrados](#)).

Diagrama de la red

Este documento utiliza la instalación de red que se muestra en el siguiente diagrama.

Configuraciones

Este documento usa las configuraciones detalladas a continuación.

Cisco 1600 Router (Cliente de 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 !--- 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-Templatel 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
```

Cisco uBR7100 CMTS (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 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-
Templatel 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
```

Verificación

En esta sección encontrará información que puede utilizar para confirmar que su configuración esté funcionando correctamente.

La herramienta [Output Interpreter](#) (sólo para clientes [registrados](#)) permite utilizar algunos comandos "show" y ver un análisis del resultado de estos comandos.

Procedimientos

Para verificar que una dirección IP se distribuye desde la agrupación LNS, siga los pasos a continuación.

1. Publique el comando **show ip local pool** del LNS. Marque la salida de comando.
LNS#show ip local pool Pool Begin End Free In use surf 100.0.0.1 100.0.0.10 9 1
2. Para identificar a la persona que llame con éxito, publique el comando **show caller ip** del LNS.
LNS#show caller ip Line User IP Address Local Number Remote Number <-> Vi29
user@surf.org 100.0.0.1 - - in
3. Para verificar la sesión VDPN en el LSN, ejecute el comando **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

Utilice los pasos abajo para verificar el número de la interfaz de plantilla virtual que está siendo utilizado por un Cliente de PPPoE.

1. Publique el comando **show vpdn session** del LAC. Marque la salida de comando.
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. Para mostrar usuarios que se han registrado con Cisco CMTS utilizando PPPoE, ejecute el comando `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. Para mostrar los dominios VPDN actuales, ejecute el comando `show vpdn domain`.
`LAC#show vpdn domain`
Tunnel VPDN Group -----
domain:surf.org2 (L2TP)

Troubleshooting

Procedimiento de Troubleshooting

Utilice las instrucciones abajo de resolver problemas su configuración.

1. Controle la LAC para verificar el estado de las interfaces por medio de la ejecución del comando `show ip interface brief`. Si las interfaces unas de los están abajo, marque el cable físico y asegúrese las interfaces no están administrativo abajo.
`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. Marque la interfaz en el PPPoE_client para verificar que la interfaz del dialer es ascendente y tiene una dirección IP del 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. Asegúrese de poder hacer ping al LNS desde el cliente 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 tiene problemas al iniciar L2TP, intente ejecutar el comando `lcp renegotiation on-mismatch` configurado en el LNS, debajo del grupo VPDN.
`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`
Nota: El (LCP) del Link Control Protocol de los proxys LAC cuando el PPP comienza. Cuando el LNS comienza a ver el PPP reenviado, observa el LCP y se queja si no encuentra lo que habría negociado con el cliente. El comando `lcp renegotiation on-mismatch` obliga al LNS a renegociar el LCP con el cliente. No todos los clientes renegociarán LCP; no obstante, la mayoría de ellos lo hacen.

Comandos para resolución de problemas

La herramienta [Output Interpreter](#) (sólo para clientes [registrados](#)) permite utilizar algunos comandos “show” y ver un análisis del resultado de estos comandos.

Nota: Antes de ejecutar un comando debug, consulte [Información Importante sobre Comandos Debug](#).

- **haga el debug de la negociación ppp** — La publicación de este comando en el LNS permite que usted vea las transacciones de la negociación PPP para identificar el problema o para efectuarlo cuando ocurre el error y desarrolla una resolución. Sin embargo, es fundamental que comprenda el resultado de debug ppp negotiation. [La comprensión de la salida de debug](#)

[ppp negotiation brinda un método exhaustivo para interpretar y solucionar problemas de PPP.](#)

- **errores del vpdn 12x-packet del debug** — lissuing este comando visualiza los errores del protocolo L2F y L2TP que previenen el establecimiento del túnel o el funcionamiento normal
- **debug vpdn 12x-packet events**—Al ejecutar este comando en el LNS, aparecen los eventos L2TP que forman parte del establecimiento o el cierre del túnel.
- **debug vpdn packet [control / data] [detail]** – ejecutando este comando en el LNS o la LAC muestra la información de encabezado del paquete de protocolo específico, tal como los números de secuencia, si los hay, indicadores, y longitud.
- **debug vpdn event [protocolo / control de flujos]** — la publicación de este comando en el LNS o el LAC visualiza los vpn errores y los eventos básicos dentro del protocolo y de los errores L2TP asociados al control de flujo donde el peer remoto recibe la ventana se configuran para un valor mayor de cero.
- **debug ppp {grieta / pap}** — la publicación de este comando visualiza el Challenge Handshake Authentication Protocol (CHAP) y el protocolo password authentication (PAP) que se incorpora al PPP.
- **debug ip udp**—Al ejecutar este comando en el LNS, se verifica el resultado a fin de determinar si los paquetes se reciben del host PPPoE.
- **debug aaa per-user**— Al ejecutar este comando desde LNS se muestran los atributos aplicados a cada usuario, a medida que el usuario realiza la autenticación.
- **radio del debug** — La publicación de este comando visualiza la información asociada cuando los usuarios autentican usando un servidor de RADIUS.

Preguntas Frecuentes

Q. ¿Cisco CMTS soporta el reenvío de PPPoE?

A. No. Los routers CMTS de Cisco no soportan el reenvío de PPPoE, que recibe los paquetes pppoe de una interfaz entrante y adelante los hacia fuera en una interfaz saliente. El Router del Cisco UBR7100 Series remite automáticamente el tráfico PPPoE cuando está configurado para el Bridging Mode del MxU (que se soporta solamente en el Cisco IOS Release 12.1 EC), sin embargo, esto es una consecuencia de la configuración de Bridging y no debido a cualquier Soporte de PPPoE. Para proporcionar la claridad, el reenvío de PPPoE no se soporta en ningún Cisco CMTS.

Q. ¿Puedo tener los Clientes de PPPoE y los clientes regulares del Protocolo de configuración dinámica de host (DHCP) al mismo tiempo en la misma planta del DOCSIS?

R. Sí. La función de terminación de PPPoE admite el uso simultáneo de clientes PPPoE y clientes DHCP detrás de los mismos CM. Los suscriptores pueden utilizar PPPoE para su registro inicial en la red de cable y luego utilizar DHCP para permitir que sus otras PC y hosts obtengan direcciones IP para acceder la red.

Q. ¿Existe soporte de PPPoE para NPE-300 y NPE-400 en las plataformas uBR7200VXR de Cisco?

R. Sí. Sin embargo, el procesador NPE-300 alcanzó su objetivo de vida útil el 15 de agosto de 2001.

Q. ¿La plataforma uBR10k CMTS de Cisco admite PPPoE?

A. No. La característica de terminación de PPPoE sólo se admite en los routers de la serie uBR7100 de Cisco y en el router uBR7246VXR de Cisco que utilizan IOS de Cisco versión 12.2(4)BC1a o posterior. No es compatible con el router uBR10012 de Cisco.

Q. ¿Cuántas sesiones PPPoE puedo funcionar con en la plataforma CMTS de Cisco?

R. La plataforma uBR hereda un límite de IDB de 10000 de la plataforma de Cisco 7200 que admite 4000 sesiones PPPoE con un NPE-225 y NPE-300, mientras que se admiten 8000 sesiones PPPoE con un NPE-400. La plataforma uBR7100 que no tiene NPE modulares, soporta 4000 sesiones PPPoE. Estos límites son teóricos. Debe considerar que la cantidad máxima de sesiones PPPoE activas y simultáneas es inferior, en función de la cantidad de memoria integrada de la tarjeta del procesador, el tipo de tarjetas de interfaz de cable utilizadas, el ancho de banda que consume cada usuario y la configuración del router.

Q. ¿Qué versión del Cisco IOS es terminación PPPoE soportó en tren de EC?

R. La característica de la terminación PPPoE no se soporta en ningún router CMTS de Cisco al usar el Cisco IOS Release 12.1 EC.

[Información Relacionada](#)

- [PPPoE Session Limit](#)
- [PPP sobre Ethernet](#)
- [PPPoE en ATM](#)
- [Cisco - Arquitectura de línea de base de PPPoE para Cisco UAC 6400](#)
- [Point-to-Point Protocol a través de la Terminación Ethernet en Cisco CMTS](#)
- [RFC 2516](#)
- [Soporte Técnico - Cisco Systems](#)