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

## Contenido



## Introducción

Este documento proporciona una configuración de ejemplo de la terminación del protocolo punto a punto sobre Ethernet (PPPoE) en una red de cable de banda ancha utilizando el Cisco uBR7100 Cable Modem Termination System (CMTS) como el Concentrador de acceso local (LAC). En este documento, un router 1600 de Cisco inicia la sesión PPPoE como cliente PPPoE, y transmite el tráfico PPP a través de una conexión de túnel de protocolo de túnel de capa dos (L2TP) seguro al servidor de red L2TP (LNS). El router LNS finaliza el túnel L2TP de Cisco CMTS y puede reenviar el tráfico a la red corporativa.

## Antes de comenzar

### Convenciones

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

### Prerequisites

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, los cablemódems compatibles con DOCSIS deben estar en línea y funcionar en el modo `Bridging`. 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 estar ejecutando la versión 12.2(4)BC1a o posterior del IOS® de Cisco. Además, para admitir la función de terminación PPPoE, el nombre de la imagen de software debe incluir el conjunto de funciones IP+ (las letras "i" y "s" deben aparecer en el nombre de la imagen de 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 equipo no incluye tal soporte, el usuario puede utilizar software cliente como WinPoet. Este documento utiliza un Cisco 1600 como el PPPoE cliente.

La información de esta configuración de laboratorio en particular se basa en las siguientes versiones de software y hardware.

- El CMTS uBR7111 de Cisco está ejecutando la versión uBR7100-ik8s-mz.122-11.BC1 del IOS de Cisco.
- El router Cisco 1600 ejecuta la versión Cisco IOS 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. All of the devices used in this document started with a cleared (default) configuration. 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. La compatibilidad de PPPoE en las interfaces de cable de los routers de las series uBR7100 y uBR7200 de Cisco permite que el equipo de las instalaciones del cliente (CPE) detrás del cable módem utilice PPP como mecanismo para obtener sus direcciones IP y utilizarlo para todo el tráfico de datos subsiguiente, similar a un cliente PPP de acceso telefónico. En una sesión de acceso telefónico PPP, la sesión PPPoE se autentica y la dirección IP se negocia entre el cliente PPPoE y el servidor, que podría 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.

PPPeE tiene dos etapas distintas, una etapa de detección y una etapa de sesión PPP. Cuando un host desea iniciar una sesión PPPoE, primero debe realizar la detección para identificar la

dirección MAC Ethernet del par y establecer un SESSION_ID PPPoE. Si bien PPP define una relación peer-to-peer, la detección es inherentemente 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.

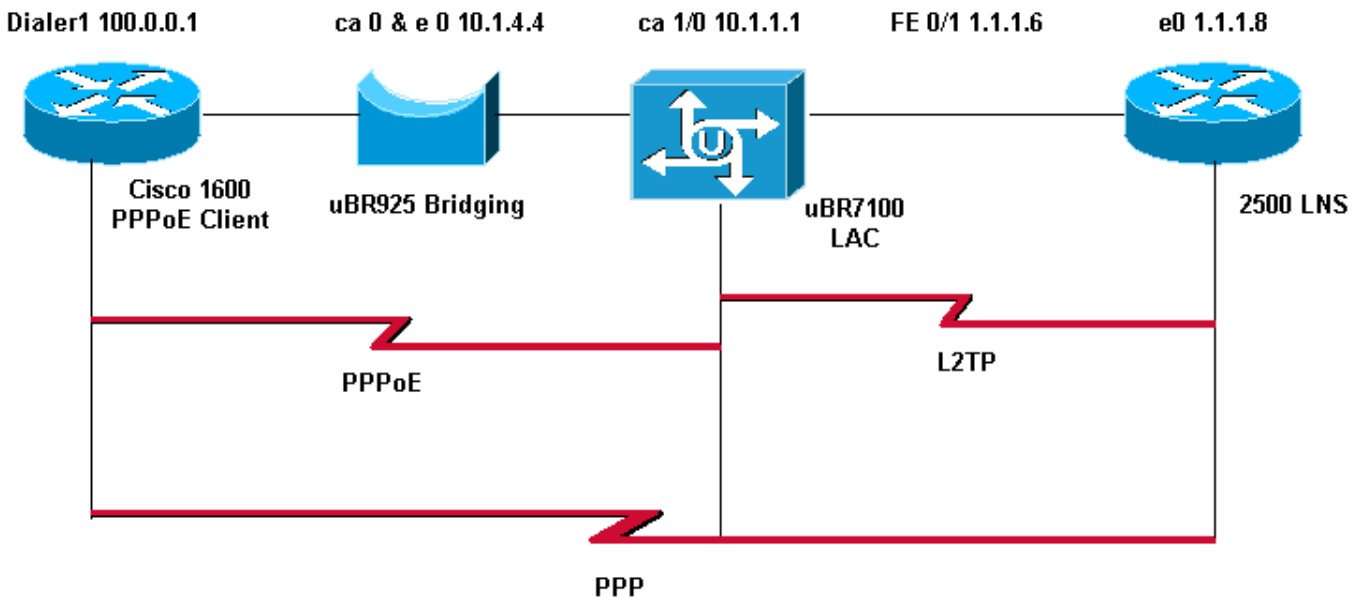
# Configurar

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

**Nota:** Para encontrar información adicional sobre los comandos usados en este documento, utilice la Command Lookup Tool (sólo 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.

**Router Cisco 1600 (cliente 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-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
```

## 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-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
```

# 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. Ejecute el comando **show ip local pool** desde el LNS. Verifique el resultado del 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 al llamador exitoso, ejecute el comando **show caller ip** desde el 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 siguientes para verificar el número de interfaz de plantilla virtual que está utilizando un cliente PPPoE.

1. Ejecute el comando **show vpdn session** desde el LAC. Verifique el resultado del 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     Ca1/0
```

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)
```

# Troubleshoot

## Procedimiento de Troubleshooting

Utilice las instrucciones que aparecen a continuación para solucionar los problemas de configuración.

1. Controle la LAC para verificar el estado de las interfaces por medio de la ejecución del comando show ip interface brief.Si alguna de las interfaces está `inactiva`, verifique el cable físico y asegúrese de que las interfaces no estén administrativamente inactivas.

```
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. Verifique la interfaz en el PPPoE_client para verificar que la interfaz del marcador esté `activa` y tenga una dirección IP del conjunto 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 protocolo de control de link (LCP) de proxy LAC cuando se inicia PPP. 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 **comandos debug**, consulte Información Importante sobre Comandos Debug.

- **debug ppp negotiation**: la ejecución de este comando en el LNS le permite ver las transacciones de negociación PPP para identificar el problema o la etapa en que se produce el error y desarrollar 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.
- **debug vpdn 12x-packet errors** : al ejecutar este comando se muestran errores de protocolo L2F y L2TP que impiden 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]* - al ejecutar este comando en el LNS o el LAC muestra información de encabezado de paquete específico del protocolo, como números de secuencia si están presentes, indicadores y longitud.
- **debug vpdn event** *[protocol* | *flow-control]* : Al ejecutar este comando en el LNS o el LAC, se muestran errores de VPN y eventos básicos dentro del protocolo L2TP y errores asociados con el control de flujo donde la ventana de recepción del par remoto se configura para un valor mayor que cero.
- **debug ppp** *{chap* | *pap}* : al ejecutar este comando, se muestran el protocolo de autenticación por desafío mutuo (CHAP) y el protocolo de autenticación por contraseña (PAP) integrados en 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.**
- **debug radius**: al ejecutar este comando, se muestra información asociada cuando los usuarios se autentican mediante un servidor RADIUS.

## Preguntas Frecuentes

**P. ¿El CMTS de Cisco admite el reenvío PPPoE?**

**A.** No. Los routers Cisco CMTS no soportan el reenvío PPPoE, que recibe paquetes PPPoE de una interfaz entrante y los reenvía en una interfaz saliente. Los routers de la serie uBR7100 de Cisco reenvían automáticamente el tráfico PPPoE cuando se configuran para el modo de conexión en puente MxU (que sólo se admite en la versión 12.1 EC del IOS de Cisco), sin embargo, esto es una consecuencia de la configuración de conexión en puente y no debido a ningún soporte PPPoE. Para proporcionar claridad, no se admite el reenvío PPPoE en ningún CMTS de Cisco.

**P. ¿Puedo tener clientes PPPoE y clientes regulares del protocolo de configuración dinámica de host (DHCP) al mismo tiempo en la misma planta DOCSIS?**

**A.** Yes. 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.

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

**A.** Yes. Sin embargo, el procesador NPE-300 alcanzó su objetivo de vida útil el 15 de agosto de 2001.

**P. ¿La plataforma uBR10k CMTS de Cisco admite PPPoE?**

**A.** No. La función de terminación PPPoE sólo se soporta en los Cisco uBR7100 Series Routers y Cisco uBR7246VXR Router, usando Cisco IOS Release 12.2(4)BC1a o posterior. No es compatible con el router uBR10012 de Cisco.

**P. ¿Cuántas sesiones PPPoE puedo ejecutar en la plataforma Cisco CMTS?**

**A.** 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.

**P. ¿Qué versión de Cisco IOS es compatible con la terminación PPPoE en el tren EC?**

**A.** La función de terminación PPPoE no se soporta en ningún router CMTS de Cisco cuando se usa Cisco IOS Release 12.1 EC.

## Información Relacionada

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