Solutions	Products	Ordering	Support	Partners	Training	Corporate

Sample Configurations

Configuring PPPoE Termination on a uBR7100 CMTS with L2TP Tunneling

Contents

Introduction

This document provides a sample configuration of Point-to-Point Protocol over Ethernet (PPPoE) termination in a broadband cable network using the Cisco uBR7100 Cable Modem Termination System (CMTS) as the Local Access Concentrator (LAC). In this document, the PPPoE session is initiated by a Cisco 1600 router as the PPPoE client, and transmits the PPP traffic through a secure Layer Two Tunneling Protocol (L2TP) tunnel connection to the L2TP Network Server (LNS). The LNS router terminates the L2TP tunnel from the Cisco CMTS, and may forward the traffic to the corporate network.

Before You Begin

Conventions

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

Prerequisites

The reader of this document should be familiar with RFC 2516 [EXIT], which describes the rules governing PPPoE, as well as the Data-over-Cable Service Interface Specifications (DOCSIS) protocol. This document does not describe how to set up the physical broadband cable network. Before attempting to configure a PPPoE solution, the DOCSIS compliant cable modems must be online and operating in `Bridging` mode. For more information on troubleshooting CMS, refer to Troubleshooting uBR Cable Modems Not Coming Online.

Components Used

The information in this document is based on the software and hardware versions below.

- The PPPoE termination feature is supported only on the Cisco uBR7100 series and Cisco uBR7246VXR universal Broadband Routers (uBR).

- The Cisco CMTS router must be running Cisco IOS® Release 12.2(4)BC1a or later release. In addition, to support the PPPoE termination feature, the software image name must include the IP+ feature set (the letters "i" and "s" must appear in the software image name).

- To support PPPoE termination on bundled cable interfaces, the Cisco CMTS router must be running Cisco IOS Release 12.2(8)BC2 or a later release.

- Client software must support the PPPoE termination protocol. If the computer operating system does not include such support, the user can use client software such as WinPoet. This document uses a Cisco 1600 as the PPPoE client.

The information in this particular lab set up is based on the software and hardware versions below.

- The Cisco uBR7111 CMTS is running Cisco IOS release uBR7100-ik8s-mz.122-11.BC1.

- The Cisco 1600 router is running Cisco IOS release Cisco 1600-sy-mz.122-11.T8.

The information presented in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If you are working in a live network, ensure that you understand the potential impact of any command before using it.

Background Theory

PPPoE provides the ability to connect a network of hosts over a simple bridging access device to a remote access concentrator. PPPoE can allow direct connection to cable interfaces. The support of PPPoE on cable interfaces of the Cisco uBR7100 and uBR7200 series routers allows Customer Premises Equipment (CPE) behind the cable modem to use PPP as a mechanism to get their IP addresses and use it for all subsequent data traffic, similar to a dial-up PPP client. In a PPP dial-up session, the PPPoE session is authenticated and the IP address is negotiated between the PPPoE client and the server, which could be either a Cisco CMTS router or a home gateway. With this model, each host utilizes its own PPP stack. Therefore, access control, billing, and type-of-service can be done on a per-user basis, rather than a per-site basis. Service providers can support both PPPoE clients and Dynamic Host Configuration Protocol (DHCP)-based hosts behind the same CM.

PPPoE has two distinct stages, a discovery stage and a PPP session stage. When a host wishes to initiate a PPPoE session, it must first perform discovery to identify the Ethernet MAC address of the peer and establish a PPPoE SESSION_ID. While PPP defines a peer-to-peer relationship, discovery is inherently a client-server relationship. In the discovery process, a host (the client) discovers an access concentrator (the server). Based on the network topology, there may be more than one access concentrator that the host can communicate with. The discovery stage allows the host to discover all access concentrators and then select one. When discovery completes successfully, both the host and the selected access concentrator have the information they will use to build their point-to-point connection over Ethernet. Once the PPPoE session begins, PPP data is sent as in any other PPP encapsulation.
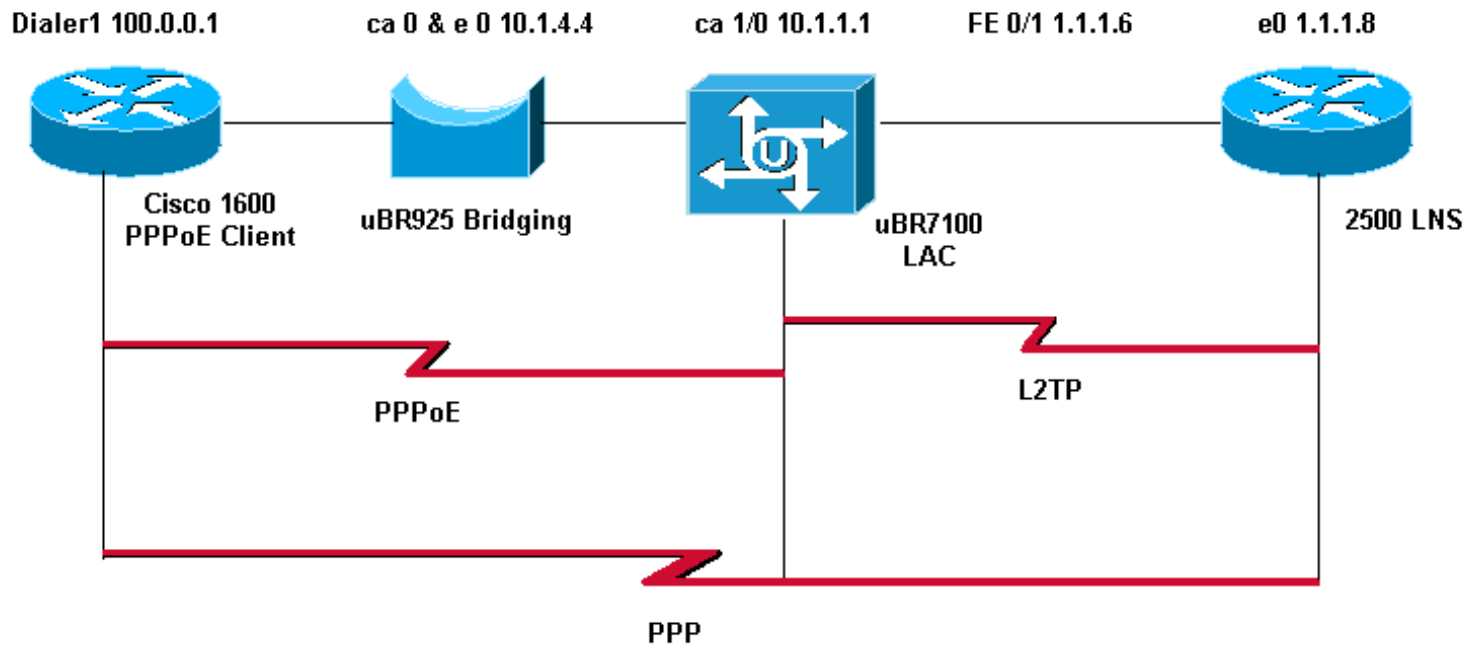
Configure

In this section, you are presented with the information to configure the features described in this document.

Note: To find additional information on the commands used in this document, use the <u>Command Lookup Tool</u> (<u>registered</u> customers only) .

Network Diagram

This document uses the network setup shown in the diagram below.

Configurations

This document uses the configurations shown below.

Cisco 1600 Router (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
```

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
```

Verify

This section provides information you can use to confirm your configuration is working properly.

Certain **show** commands are supported by the Output Interpreter Tool (registered customers only) , which allows you to view an analysis of **show** command output.

Procedures

To verify that an IP address is being handed out from the LNS pool, follow the steps below.

1. Issue the **show ip local pool** command from the LNS. Check the command output.

   ```
   LNS#show ip local pool

    Pool                     Begin            End                Free      In use
    surf                     100.0.0.1        100.0.0.10          9          1
   ```

2. To identify the successful caller, issue the **show caller ip** command from the LNS.

   ```
   LNS#show caller ip

     Line          User                         IP Address      Local Number      Remote
     Number   <->
     Vi29          user@surf.org                100.0.0.1            -                  -
     in
   ```

3. To verify the VPDN session on the LNS, issue the **show vpdn session** command.

   ```
   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
```

Use the steps below to verify the virtual-template interface number that is being used by a PPPoE client.

1. Issue the **show vpdn session** command from the LAC. Check the command output.

```
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. To display users who have registered with the Cisco CMTS using PPPoE, issue the **show interface cable modem** command.

```
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. To display the current VPDN domains, issue the **show vpdn domain** command.

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

Troubleshoot

Troubleshooting Procedure

Use the instructions below to troubleshoot your configuration.

1. Check on the LAC to see the status of the interfaces by issuing the **show ip interface brief** command.

   If any of the interfaces are down, check the physical cable and make sure the interfaces are not administratively down.

```
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. Check the interface on the PPPoE_client to verify that the dialer interface is up and has an IP address from the LNS pool.

```
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. Make sure that you can ping the LNS from the 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. If you are having problems initiating L2TP, try issuing the **lcp renegotiation on-mismatch** command configured on the LNS under 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
```

Note: The LAC proxies Link Control Protocol (LCP) when PPP starts. When the LNS begins seeing the forwarded PPP, it looks at the LCP and if it is not what it would have negotiated with the client itself, it complains. The **lcp renegotiation on-mismatch** command forces the LNS to renegotiate LCP with the client. Not all clients will renegotiate LCP, however, most of them do.

Troubleshooting Commands

Certain **show** commands are supported by the [Output Interpreter Tool](#) ([registered](#) customers only) , which allows you to view an analysis of **show** command output.

Note: Before issuing **debug** commands, please see [Important Information on Debug Commands](#).

- **debug ppp negotiation** — Issuing this command on the LNS allows you to view the PPP negotiation transactions to identify the problem or stage when the error occurs and develop a resolution. It is imperative, however, that you understand the **debug ppp negotiation** output. [Understanding debug ppp negotiation Output](#) provides a comprehensive method for reading and troubleshooting PPP.

- **debug vpdn 12x-packet errors**— Iissuing this command displays L2F and L2TP protocol errors that prevent tunnel establishment or normal operation

- **debug vpdn 12x-packet events**— Issuing this command on the LNS displays L2TP events that are part of tunnel establishment or shutdown.

- **debug vpdn packet** *[control | data] [detail]* - issuing this command on the LNS or the LAC displays protocol-specific packet header information, such as sequence numbers if present, flags, and length.

- **debug vpdn event** *[protocol | flow-control]* — Issuing this command on the LNS or the LAC displays VPN errors and basic events within the L2TP protocol and errors associated with flow control where the remote peer receive window is configured for a value greater than zero.

- **debug ppp** *{chap | pap}* — Issuing this command displays the Challenge Handshake Authentication Protocol (CHAP) and Password Authentication Protocol (PAP) that is built into PPP.

- **debug ip udp**— Issuing this command on the LNS checks the output to see whether packets are being received from the pppoe host.

- **debug aaa per-user**— Issuing this command from the LNS displays what attributes are applied to each user as the user authenticates.

- **debug radius**— Issuing this command displays information associated when users authenticate using a RADIUS server.

Frequently Asked Questions

Q. Does the Cisco CMTS support PPPoE forwarding?

A. No. The Cisco CMTS routers do not support PPPoE forwarding, which receives PPPoE packets from an incoming interface and forwards them out on an outgoing interface. The Cisco uBR7100 series routers do automatically forward PPPoE traffic when configured for MxU bridging mode (which is supported only on Cisco IOS Release 12.1 EC), however, this is a consequence of the bridging configuration and not due to any PPPoE support. To provide clarity, PPPoE Forwarding is not supported on any Cisco CMTS.

Q. Can I have PPPoE clients and regular Dynamic Host Configuration Protocol (DHCP) clients at the same time on the same DOCSIS plant?

A. Yes. The PPPoE termination feature supports simultaneous use of PPPoE clients and DHCP clients behind the same CMs. Subscribers can use PPPoE for their initial log on to the cable network, and then use DHCP to allow their other PCs and other hosts to obtain IP addresses for network access.

Q. Is there PPPoE support for both the NPE-300 and NPE-400 on the Cisco uBR7200VXR CMTS platforms?

A. Yes. The NPE-300 processor reached its end-of-life milestone on August 15, 2001, however.

Q. Is PPPoE supported on the Cisco uBR10k CMTS platform?

A. No. The PPPoE termination feature is only supported on the Cisco uBR7100 series routers and Cisco uBR7246VXR router, using Cisco IOS Release 12.2(4)BC1a or later. It is not supported on the Cisco uBR10012 router.

Q. How many PPPoE sessions can I run on the Cisco CMTS platform?

A. The uBR platform inherits an IDB limit of 10000 from the the cisco 7200 platform which supports 4000 PPPoE sessions with a NPE-225 and NPE-300 while 8000 PPPoE sessions are supported with a NPE-400. The uBR7100 platform which does not have have modular NPEs, supports 4000 PPPoE sessions. These are theoretical limits. You must consider that the maximum number of active, simultaneous PPPoE sessions is less, depending on the amount of memory onboard the processor card, the type of cable interface cards being used, the bandwidth being consumed by each user, and the router's configuration.

Q. What release of Cisco IOS is PPPoE termination supported in the EC train?

A. The PPPoE termination feature is not supported on any Cisco CMTS router when using Cisco IOS Release 12.1 EC.

Related Information

- **PPPoE Session Limit**
- **PPP over Ethernet**
- **PPPoE on ATM**
- **Cisco - PPPoE Baseline Architecture for the Cisco UAC 6400**

- **Point-to-Point Protocol over Ethernet Termination on the Cisco CMTS**

- **RFC 2516**

- **Technical Support - Cisco Systems**

| Home | How to Buy | Login | Profile | Feedback | Site Map | Help |