CHAPTER 14

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

Revised: February 5, 2007, OL-1467-08

This chapter describes the PPPoE Termination feature, which allows service providers to extend their existing PPP dial-up provisioning systems to users on cable networks by encapsulating the PPP packets within Ethernet MAC frames.

Feature Specifications for PPPoE Termination

Feature History	
Release	**Modification**
Release 12.1(5)T	This feature was introduced for the Cisco uBR7200 series routers. **Note** The Cisco IOS Release 12.1T and 12.2T trains are no longer supported for the Cisco uBR7200 series routers.
Release 12.2(4)BC1a	This feature was supported on the 12.2BC train for the Cisco uBR7100 series and Cisco uBR7246VXR routers.
Release 12.2(8)BC1	Support was added for SNMP support with the CISCO-PPPOE-MIB.
Release 12.2(8)BC2	Support was added for bundled cable interfaces.
Supported Platforms	
Cisco uBR7100 series, Cisco uBR7246VXR router	

Note The PPPoE Termination feature is not supported on the Cisco uBR10012 universal broadband router in any Cisco IOS software release. The PPPoE Termination is also not supported on any Cisco CMTS router when running Cisco IOS Release 12.1 EC.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

This document includes the following major sections:

Prerequisites for PPPoE Termination

The PPPoE Termination feature has the following prerequisites:

- The PPPoE Termination feature is supported only on the Cisco uBR7100 series and Cisco uBR7246VXR universal broadband routers.
- 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 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.
- If planning on a large number of PPPoE sessions and traffic, increase the size of the packet hold queues on the WAN interfaces (ATM, DPT, Gigabit Ethernet, etc.), using the **hold-queue** *packet-size* {**in** | **out**} command. For example:

```
Router(config)# interface gigabitethernet 1/0
Router(config-if)# hold-queue 4096 in
Router(config-if)# hold-queue 4096 out
Router(config-if)#
```

Restrictions for PPPoE Termination

The PPPoE Termination feature has the following restrictions and limitations:

- 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.
- The PPPoE Termination feature is not supported on any Cisco CMTS router when using Cisco IOS Release 12.1 EC.
- PPPoE Forwarding is not supported on any Cisco CMTS.
- Table 14-1 shows the absolute maximum number of PPPoE sessions supported on the Cisco uBR7100 series routers, and on the Cisco uBR7246VXR router when using different processor cards.

Table 14-1 Absolute Maximum Number of PPPoE Sessions

Processor	Absolute Maximum Number of PPPoE Sessions
Cisco uBR7100 series	4000
NPE-225	4000
NPE-300[1]	4000
NPE-400	8000
NPE-G1	10000

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

Note The maximum number of active, simultaneous PPPoE sessions is much less (approximately 600 to 800), depending on the number of 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.

Information About PPPoE Termination

This section describes the PPPoE Termination feature:

Feature Overview

The Point-to-Point Protocol over Ethernet (PPPoE) feature supports PPPoE on cable interfaces, allowing service providers to extend their existing PPP dial-up provisioning systems to users on cable networks. When PPPoE Termination is enabled, the Cisco CMTS encapsulates PPP packets in Ethernet frames within PPPoE sessions.

When the Cisco CMTS receives PPPoE traffic from PPPoE sessions that are initiated by the user's PC, the Cisco CMTS either terminates the PPPoE sessions on the cable interface or transmits the PPPoE traffic through a secure tunnel connection, depending on the Cisco CMTS configuration. The following are the most typical configurations:

- Internet access—For residential customers and other users who want only basic Internet access, traffic is sent out on the WAN interface as standard IP packets. The service provider can use the same provisioning systems as they use for their dial-up users and other broadband users. The PPPoE session exists only between the cable modem and Cisco CMTS, simplifying network management and configuration.
- Secure corporate access—For businesses or telecommuters, traffic is forwarded over a Layer 2 point-to-point Tunneling Protocol (L2TP) tunnel to a L2TP network server (LNS) to create secure corporate intranet access. Cable modem users can access company resources as if they were directly connected to the corporate network, without compromising network security. This tunnel can be built over whatever interface is being used with the corporate site (Ethernet, ATM, and so forth).

When using the L2TP tunnel configuration, the Cisco CMTS acts as the L2TP Access Concentrator (LAC), or Network Access Server (NAS). The endpoint of the tunnel is the LNS, which can be a router such as a Cisco 6400 Carrier-Class Broadband Aggregator.

When the cable modem, acting as a bridge, receives its PPPoE session traffic, it forwards the traffic on to the hosts and other customer premises equipment (CPE) devices that are connected behind it. Users at these hosts or CPE devices can use standard PPP to log on to the cable network and obtain their IP addresses and other network information. Users can automate this procedure by using a router that supports PPPoE or by using standard PPPoE software, such as WinPoet.

User names and passwords can be included in the Cisco CMTS configuration, or the service provider can use the same Remote Authentication Dial-In User Service (RADIUS) authentication servers as they use for their dial-up and digital subscriber line (DSL) users. For example, the Cisco Subscriber Registration Center (CSRC) provides an Access Registrar that provides RADIUS server authentication.

The PPPoE Termination feature supports simultaneous use of PPPoE clients and Dynamic Host Configuration Protocol (DHCP) clients behind the same cable modems. 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.

Note 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), but this is a consequence of the bridging configuration and not due to any PPPoE support.

Benefits

The PPPoE Termination feature provides the following benefits to cable service providers and their partners and customers:

- PPPoE complements and does not interfere with the standard DOCSIS registration and authentication procedures that are used for cable modems.
- PPPoE can be used on existing customer premise equipment, by extending the PPP session over the bridged Ethernet LAN to the PC (host).
- PPPoE preserves the point-to-point session used by ISPs in a dial-up model, without requiring an intermediate set of IP communications protocols.
- Service providers can use their existing dial-up PPP provisioning and authentication systems for users on the cable network.
- PPPoE supports the security features, such as Challenge Handshake Authentication Protocol (CHAP) and Password Authentication Protocol (PAP), that are built into PPP systems.
- Service providers can support both PPPoE clients and DHCP-based hosts behind the same cable modem.

How to Configure the PPPoE Termination Feature

This section describes the following tasks that are needed to implement the PPPoE Termination feature. All procedures are required, depending on the router's configuration.

Enabling VPDN Operations on the Cisco CMTS

Use the following commands, starting in user EXEC mode, to enable virtual private dialup network (VPDN) operations on the Cisco CMTS router that is acting an L2TP access concentrator (LAC). This procedure must be done before performing any of the other configuration procedures.

Note This procedure also must be performed on the Cisco router that is acting as the L2TP network server (LNS).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **buffers small** {**initial** | **max-free** | **permanent**} **1024**
4. **vpdn enable**
5. **vpdn logging**
6. **username** *user-name* **password** {0 | 7} *password*
7. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**enable**
	
	Example:
	`Router> enable`
	`Router#`
		Enables privileged EXEC mode. Enter your password if prompted.

Step 2	**configure terminal**
	
	Example:
	`Router# configure terminal`
	`Router(config)#`
		Enters global configuration mode.

Step 3	**buffers small** {**initial** | **max-free** | **permanent**} **1024**
	
	Example:
	`Router(config)# buffers small initial 1024`
	`Router(config)# buffers small max-free 1024`
	`Router(config)# buffers small permanent 1024`
	`Router(config)#`
		(Optional) Increases the size of the buffers on the router that are used for small packets to account for the larger number of keepalive packets that are sent during PPPoE sessions.
		
		Note Repeat this command for each type of small packet buffers.

Step 4	**vpdn enable**
	
	Example:
	`Router(config)# vpdn enable`
	`Router(config)#`
		Enables virtual private dial-up networking (VPDN).

Step 5	**vpdn logging**
	
	Example:
	`Router(config)# vpdn logging`
	`Router(config)#`
		(Optional) Enable logging for VPDN operations. Logging is automatically disabled by default (**no vpdn logging**) when you enable VPDN. Use this command to enable logging.

Step 6	**username** *user-name* **password** [*level*] *password*
	
	Example:
	`Router(config)# username pppoe-user1@client.com password 0 pppoepassword`
	`Router(config)#`
		Specifies a username and password for each user to be granted PPPoE access:
		• *user-name* = Username that the user uses to log in.
		• *level* = (Optional) Encryption level for the password. The valid values are 0 (default, the following password is not encrypted) and 7 (the following password is encrypted—this option is typically used only when cutting and pasting configurations from other routers).
		• *password* = Password that the above user must use to log in and create a PPPoE user session.
		
		Note This step is not required if you are using an external server, such as a RADIUS server, to perform user authentication.

	Command or Action	Purpose

Step 7	`exit`
	
	Example:
	`Router(config)# exit`
	`Router#`
		Exits global configuration mode.

Configuring a Virtual Template on the Cisco CMTS

Use the following commands, starting in user EXEC mode, to create and configure a virtual template on the Cisco CMTS router when it is acting as a LAC. This procedure is required because the Cisco CMTS uses the virtual template to configure the virtual interfaces it creates for each individual PPPoE session.

Note At least one virtual template must be created on the router to support PPPoE sessions from cable modem users.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface virtual-template** *number*
4. **ip unnumbered** *interface*
5. **ip mtu 1492**
6. **keepalive** [*period* [*retries*]]
7. **peer default ip address pool** *name*
8. **ppp authentication** {**chap** | **ms-chap** | **pap**}
9. **ppp timeout authentication** *response-time*
10. **ppp timeout retry** *timeout*
11. **no logging event link-status**
12. **no cdp enable**
13. **exit**
14. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**enable**
	
	Example:
	`Router> enable`
	`Router#`
		Enables privileged EXEC mode. Enter your password if prompted.

Step 2	**configure terminal**
	
	Example:
	`Router# configure terminal`
	`Router(config)#`
		Enters global configuration mode.

Step 3	**interface virtual-template** *number*
	
	Example:
	`Router(config)# interface virtual-template 1`
	`Router(config-if)#`
		Select the number of the virtual-template interface to be configured and enters interface configuration mode.
		
		Note You can create up to 200 virtual interfaces on each router.

Step 4	**ip unnumbered** *interface*
	
	Example:
	`Router(config-if)# ip unnumbered Ethernet2/0`
	`Router(config-if)#`
		Enables the virtual template interfaces to process IP packets by using the IP address of the specified interface, as opposed to assigning a unique IP address to each virtual interface.

Step 5	**ip mtu 1492**
	
	Example:
	`Router(config-if)# ip mtu 1492`
	`Router(config-if)#`
		Configures the maximum transmission unit (MTU) size to 1492 bytes to allow for the eight additional header bytes used by the PPP and PPPoE encapsulation.

Step 6	**keepalive** *period* [*retries*]
	
	Example:
	`Router(config-if)# keepalive 60 10`
	`Router(config-if)#`
		(Optional) Specifies how often and how many times the router should send keepalive messages on the virtual interface without receiving a response before bringing down the tunnel protocol and ending that particular PPPoE session.
		• *period* = Specifies how long, in seconds, the router should send a keepalive message and wait for a response. The valid range is 0 to 32767 seconds, with a default of 10.
		• *retries* = (Optional) Specifies the number of times the router will resend a keepalive packet without receiving a response. The valid range is 1 to 255, with a default of 5.
		
		Note Increasing the keepalive period and number of retries might be necessary when supporting a large number of PPPoE sessions.

	Command or Action	Purpose

Step 7	**peer default ip address pool** *name* [*name2* ...]
	
	Example:
	`Router(config-if)# peer default ip address pool local`
	`Router(config-if)#`
		(Optional) Defines one or more pools of addresses to be used when assigning IP addresses to the PPPoE clients.

Step 8	**ppp authentication** {**chap** | **ms-chap** | **pap**}
	
	Example:
	`Router(config-if)# ppp authentication chap`
	`Router(config-if)#`
		Defines the authentication method to be used for PPPoE sessions:
		• **chap** = Challenge Handshake Authentication Protocol
		• **ms-chap** = Microsoft's version of CHAP
		• **pap** = Password Authentication Protocol

Step 9	**ppp timeout authentication** *response-time*
	
	Example:
	`Router(config-if)# ppp timeout authentication 10`
	`Router(config-if)#`
		(Optional) Specifies the maximum time, in seconds, that the router should wait for a response to a PPP authentication packet. The valid range is 0 to 255 seconds, with a default of 10 seconds.
		Note Increase this timeout if PPPoE sessions begin failing due to timeout errors.

Step 10	**ppp timeout retry** *timeout*
	
	Example:
	`Router(config-if)# ppp timeout retry 5`
	`Router(config-if)#`
		(Optional) Specifies the maximum time, in seconds, that the router should wait for a response during PPP negotiation. The valid range is 1 to 255 seconds, with a default of 2 seconds.
		Note Increase this timeout if PPPoE sessions begin failing due to timeout errors.

Step 11	**no logging event link-status**
	
	Example:
	`Router(config-if)# no logging event link-status`
	`Router(config-if)#`
		(Optional) Disables sending unnecessary link up and link down event messages to the router's event log. These messages would otherwise be sent each time a PPPoE session begins and ends.

Step 12	**no cdp enable**
	
	Example:
	`Router(config-if)# no cdp enable`
	`Router(config-if)#`
		(Optional) Disables the use of the Cisco Discovery Protocol (CDP) on the virtual interface. This protocol is unnecessary on a virtual interface for PPPoE sessions.

Step 13	**exit**
	
	Example:
	`Router(config-if)# exit`
	`Router(config)#`
		Exits interface configuration mode.

Step 14	**exit**
	
	Example:
	`Router(config)# exit`
	`Router#`
		Exits global configuration mode.

Configuring a VPDN Group for PPPoE Sessions

Use the following commands, starting in user EXEC mode, to create and configure a virtual private dialup network (VPDN) group on the Cisco CMTS router that is acting an L2TP access concentrator (LAC). The router uses the VPDN group to configure the PPPoE sessions it creates for cable modem users. This step is required on the Cisco CMTS.

Note You can create only one VPDN group to support PPPoE sessions.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn-group** *number*
4. **accept-dialin**
5. **protocol pppoe**
6. **virtual-template** *number*
7. **exit**
8. **lcp renegotiation** {**always** | **on-mismatch**}
9. **pppoe limit per-mac** *number*
10. **pppoe limit max-sessions** *number-of-sessions* [**threshold-sessions** *number*]
11. **exit**
12. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**enable**
	
	Example:
	`Router> enable`
	`Router#`
		Enables privileged EXEC mode. Enter your password if prompted.

Step 2	**configure terminal**
	
	Example:
	`Router# configure terminal`
	`Router(config)#`
		Enters global configuration mode.

Step 3	**vpdn-group** *name*
	
	Example:
	`Router(config)# vpdn-group 1`
	`Router(config-vpdn)#`
		Creates a VPDN group with the specified name or number and enters VPDN-group configuration mode.

	Command or Action	Purpose

Step 4	`Router(config-vpdn)# accept-dialin`
	
	Example:
	`Router(config-vpdn)# accept-dialin`
	`Router(config-vpdn-acc-in)#`
		Configures the router to accept tunneled PPP/PPPoE connections from the LAC and enters VPDN accept dialin configuration mode.

Step 5	`Router(config-vpdn)# protocol pppoe`
	
	Example:
	`Router(config-vpdn)# protocol pppoe`
	`Router(config-vpdn-acc-in)#`
		Configures the VPDN group to use the PPPoE protocol.

Step 6	**virtual-template** *number*
	
	Example:
	`Router(config-vpdn-acc-in)# virtual-template 1`
	`Router(config-vpdn-acc-in)#`
		Specifies the number of the virtual-interface template to be used when configuring a PPPoE session.
		
		Note This should be the same virtual-interface template defined in Configuring a Virtual Template on the Cisco CMTS, page 14-7.

Step 7	**exit**
	
	Example:
	`Router(config-vpdn-acc-in)# exit`
	`Router(config-vpdn)#`
		Exits VPDN accept dialin configuration mode.

Step 8	**lcp renegotiation** {**always** | **on-mismatch**}
	
	Example:
	`Router(config-vpdn)# lcp renegotiation always`
	`Router(config-vpdn)#`
		(Optional) Specifies whether the Cisco CMTS, acting as the LNS, can renegotiate the PPP Link Control Protocol (LCP) with the router acting as the LAC:
		• **always** = Always allows the Cisco CMTS to renegotiate the connection.
		• **on-mismatch** = The Cisco CMTS can renegotiate the connection only when a configuration mismatch is discovered between the LNS and LAC.
		The default is that the LNS should not be able to renegotiate the connection.

Step 9	**pppoe limit per-mac** *number*
	
	Example:
	`Router(config-vpdn)# pppoe limit per-mac 1`
	`Router(config-vpdn)#`
		(Optional) Specifies the maximum number of PPPoE sessions that can originate from each MAC address. The valid range is 1 to 5000, with a default of 100. For cable users, Cisco recommends a maximum of 1 PPPoE session per MAC address.
		
		Note This command is not available until after you have configured the group for the PPPoE protocol in Step 5.

	Command or Action	Purpose

Step 10	**pppoe limit max-sessions** *number-of-sessions* [**threshold-sessions** *number*]
	
	Example:
	`Router(config-vpdn)# pppoe limit max-sessions 1000 threshold-sessions 750`
	`Router(config-vpdn)#`
		(Optional) Specifies the number of PPPoE sessions supported on the router:
		• *number* = Specifies the maximum number of PPPoE sessions that can be established at any one time on the router. The valid range is 1 to 5000, with a default of 100.
		• **threshold-sessions** *number* = (Optional) Specifies the threshold for active PPPoE sessions. If the number of sessions exceeds this value, an SNMP trap can be sent. The valid range is 1 to 5000, and the default equals the *number-of-sessions* value.
		Note This command is not available until after you have configured the group for the PPPoE protocol in Step 5.

Step 11	**exit**
	
	Example:
	`Router(config-vpdn)# exit`
	`Router(config)#`
		Exits VPDN-group configuration mode.

Step 12	**exit**
	
	Example:
	`Router(config)# exit`
	`Router#`
		Exits global configuration mode.

Configuring a VPDN Group for L2TP Tunnel Initiation on the Cisco CMTS

Use the following commands, starting in user EXEC mode, to create and configure a virtual private dialup network (VPDN) group on the Cisco CMTS router that is acting as a when it is acting an L2TP access concentrator (LAC), so that it can create an L2TP tunnel with the L2TP network server (LNS).

Note This step is required when you are using L2TP tunneling with PPPoE sessions. In this configuration, you must create at least one VPDN group to support the PPPoE sessions and at least one other VPDN group to support the L2TP tunnel.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn-group** *number*
4. **request-dialin**
5. **protocol l2tp**
6. **domain** *domain-name*
7. **exit**

8. **initiate-to ip** *ip-address*
9. **local name** *pppoe-username*
10. **no l2tp tunnel authentication**
11. **exit**
12. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**enable**
	
	Example:
	`Router> enable`
	`Router#`
		Enables privileged EXEC mode. Enter your password if prompted.

Step 2	**configure terminal**
	
	Example:
	`Router# configure terminal`
	`Router(config)#`
		Enters global configuration mode.

Step 3	**vpdn-group** *number*
	
	Example:
	`Router(config)# vpdn-group 2`
	`Router(config-vpdn)#`
		Creates the VPDN group with the specified number and enters VPDN-group configuration mode.

Step 4	`Router(config-vpdn)#` **request-dialin**
	
	Example:
	`Router(config-vpdn)# request-dialin`
	`Router(config-vpdn-req-in)#`
		Configures the router to initiate L2TP tunnel requests and enters VPDN request dialin configuration mode.

Step 5	**protocol l2tp**
	
	Example:
	`Router(config-vpdn-req-in)# protocol l2tp`
	`Router(config-vpdn-req-in)#`
		Configures the VPDN group for the L2TP protocol.

Step 6	**domain** *domain-name*
	
	Example:
	`Router(config-vpdn-req-in)# domain client.com`
	`Router(config-vpdn-req-in)#`
		Specifies that this VPDN group should be used to create PPPoE sessions for clients requesting access from the specified domain name.

Step 7	**exit**
	
	`Example:`
	`Router(config-vpdn-req-in)# exit`
	`Router(config-vpdn)#`
		Exits VPDN request dialin configuration mode.

	Command or Action	Purpose

Step 8	**initiate-to ip** *ip-address*
	
	Example:
	`Router(config-vpdn)# initiate-to ip 10.10.10.2`
	`Router(config-vpdn)#`
		Establishes the IP address for the termination point of the L2TP tunnel that is used by PPPoE clients using this VPDN group.

Step 9	**local name** *pppoe-username*
	
	Example:
	`Router(config-vpdn)# local name PpPoE-UsER`
	`Router(config-vpdn)#`
		Specifies the username to be used for authentication on the VPDN group.

Step 10	**no l2tp tunnel authentication**
	
	Example:
	`Router(config-vpdn)# no l2tp tunnel authentication`
	`Router(config-vpdn)#`
		Disables authentication for the creation of the L2TP tunnel (but continues to authenticate individual user sessions).

Step 11	**exit**
	
	Example:
	`Router(config-vpdn)# exit`
	`Router(config)#`
		Exits VPDN-group configuration mode.

Step 12	**exit**
	
	Example:
	`Router(config)# exit`
	`Router#`
		Exits global configuration mode.

Enabling PPPoE on a Cable Interface

Use the following commands, starting in user EXEC mode, to enable PPPoE on a specific cable interface on the Cisco CMTS router when it is acting an L2TP access concentrator (LAC).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface cable** *x/y*
4. **pppoe enable**
5. **hold-queue** *n* **in**
6. **hold-queue** *n* **out**
7. **exit**
8. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**enable**
	
	Example:
	`Router> enable`
	`Router#`
		Enables privileged EXEC mode. Enter your password if prompted.

Step 2	**configure terminal**
	
	Example:
	`Router# configure terminal`
	`Router(config)#`
		Enters global configuration mode.

Step 3	**interface cable** *x/y*
	
	Example:
	`Router(config)# interface cable 4/0`
	`Router(config-if)#`
		Enters cable interface configuration mode for the specified cable interface:

Step 4	**pppoe enable**
	
	Example:
	`Router(config-if)# pppoe enable`
	`Router(config-if)#`
		Enables PPPoE on the interface, allowing PPPoE sessions to be created through that interface. (The **pppoe enable** command is not available until you enable VPDN operations, using the **vpdn enable** command as shown in the procedure given in the "Enabling VPDN Operations on the Cisco CMTS" section on page 14-5.)
		Note Enabling PPPoE on a cable interface also automatically enables it on all subinterfaces.

Step 5	**hold-queue** *n* **in**
	
	Example:
	`Router(config-if)# hold-queue 1000 in`
	`Router(config-if)#`
		(Optional) Specify the maximum number of data packets that can be stored in the input queue during PPPoE sessions. The valid range is 0 to 65535 packets, with a default of 75.
		Note To support a large number of simultaneous PPPoE sessions, set the input queue value to at least 1000 packets to avoid dropped packets.

Step 6	**hold-queue** *n* **out**
	
	Example:
	`Router(config-if)# hold-queue 1000 out`
	`Router(config-if)#`
		(Optional) Specify the maximum number of data packets that can be stored in the output queue during PPPoE sessions. The valid range is 0 to 65535 packets, with a default of 40.
		Note To support a large number of simultaneous PPPoE sessions, set the output queue value to at least 1000 packets to avoid dropped packets.

	Note Repeat Step 3 through Step 6 for each cable interface that supports PPPoE sessions.	

	Command or Action	Purpose

Step 7	**exit**
	
	Example:
	`Router(config-if)# exit`
	`Router(config)#`
		Exits interface configuration mode.

Step 8	**exit**
	
	Example:
	`Router(config)# exit`
	`Router#`
		Exits global configuration mode.

Configuring a Cisco Router as LNS

Use the following commands, starting in user EXEC mode, to enable and configure a Cisco router, such as the Cisco 6400, to act as the L2TP network server (LNS), so that it can terminate the L2TP tunnels initiated by the Cisco CMTS router when it is acting an L2TP access concentrator (LAC).

Note Before performing this procedure on the LNS router, you must also enable VPDN operations, using the procedure given in the "Enabling VPDN Operations on the Cisco CMTS" section on page 14-5. In addition, you must also create and configure a virtual-interface template, using the procedure given in the "Configuring a Virtual Template on the Cisco CMTS" section on page 14-7.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn-group** *number*
4. **accept-dialin**
5. **protocol l2tp**
6. **virtual-template** *number*
7. **exit**
8. **terminate-from hostname** *hostname*
9. **no l2tp tunnel authentication**
10. **exit**
11. **virtual-template** *number* **pre-clone** *number*
12. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**enable**
	
	Example:
	`Router> enable`
	`Router#`
		Enables privileged EXEC mode. Enter your password if prompted.

Step 2	**configure terminal**
	
	Example:
	`Router# configure terminal`
	`Router(config)#`
		Enters global configuration mode.

Step 3	**vpdn-group** *number*
	
	Example:
	`Router(config)# vpdn-group 1`
	`Router(config-vpdn)#`
		Select the VPDN group number and enters VPDN-group configuration mode.

Step 4	**accept-dialin**
	
	Example:
	`Router(config-vpdn)# accept-dialin`
	`Router(config-config-vpdn-acc-in)#`
		Configures the router to accept dial-in calls and enters VPDN accept dialin configuration mode.

Step 5	**protocol l2tp**
	
	Example:
	`Router(config-vpdn-acc-in)# protocol pppoe`
	`Router(config-vpdn-acc-in)#`
		Configures the VPDN group for the L2TP protocol so that it can access the PPPoE server.

Step 6	**virtual-template** *number*
	
	Example:
	`Router(config-vpdn-acc-in)# virtual-template 1`
	`Router(config-vpdn-acc-in)#`
		Specifies the number of the virtual-interface template to be used when configuring a PPPoE session.
		
		Note Specify the number of a virtual-interface template that has been created using the procedure given in the "Configuring a Virtual Template on the Cisco CMTS" section on page 14-7.

Step 7	**exit**
	
	Example:
	`Router(config-vpdn-acc-in)# exit`
	`Router(config-vpdn)#`
		Exits VPDN accept dialin configuration mode.

Step 8	**terminate-from hostname** *hostname*
	
	Example:
	`Router(config-vpdn)# terminate-from hostname ciscocmts-router`
	`Router(config-vpdn)#`
		Configures this group so that it terminates L2TP tunnels from the specified hostname. The *hostname* should be the host name for the Cisco CMTS that is configured for PPPoE termination.

	Command or Action	Purpose

Step 9	**no l2tp tunnel authentication**
	
	Example:
	`Router(config-vpdn)# no l2tp tunnel authentication`
	`Router(config-vpdn)#`
		Disables authentication for the creation of the L2TP tunnel (but continues to authenticate individual user sessions).

Step 10	**exit**
	
	Example:
	`Router(config-vpdn)# exit`
	`Router(config)#`
		Exits VPDN-group configuration mode.

Step 11	**virtual-template** *number* **pre-clone** *number*
	
	Example:
	`Router(config)# virtual-template 1 pre-clone 2000`
	`Router(config)#`
		(Optional) Creates the specified number of virtual interfaces in advance, which can speed up the bring up of individual sessions and reduce the load on the router's processor when a large number of sessions come online at the same time.
		• *number* = Number of virtual interfaces to be created in advance. This value should match the total number of PPPoE sessions that the router is expected to support.
		Note Pre-cloning is not recommended when using virtual subinterfaces.

Step 12	**exit**
	
	Example:
	`Router(config)# exit`
	`Router#`
		Exits global configuration mode.

Clearing PPPoE Sessions

To clear all PPPoE sessions for a particular MAC address, use the **clear cable host** command:

```
Router# clear cable host mac-address
Router#
```

The following example shows a PPPoE session for a particular host being cleared:

```
Router# show interface c3/0 modem 0

SID   Priv bits  Type      State       IP address      method    MAC address
1     00         modem     offline     3.18.1.5        dhcp      0030.80bc.2303
1     00         host      offline                     pppoe     0010.2937.b254

Router# clear cable host 0010.2937.b254

Router# show interface c3/0 modem 0

SID   Priv bits  Type      State       IP address      method    MAC address
1     00         modem     offline     3.18.1.5        dhcp      0030.80bc.2303

Router#
```

Enabling SNMP Traps for Active PPPoE Sessions

In Cisco IOS Release 12.2(8)BC1 and later releases, you can enable SNMP traps to inform you when the number of active PPPoE sessions exceeds a threshold value, using the following procedure.

Note Configure the threshold value using the **threshold-sessions** option for the **pppoe limit max-sessions** command when configuring the VPDN group for PPPoE sessions. For more information about PPPoE traps, see the CISCO-PPPOE-MIB.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps pppoe**
4. **exit**

Note To enable SNMP traps, you must also configure the router to support SNMP sessions and specify at least one SNMP manager to receive the SNMP traps.

DETAILED STEPS

	Command or Action	Purpose

Step 1	**enable**
	
	Example:
	`Router> enable`
	`Router#`
		Enables privileged EXEC mode. Enter your password if prompted.

Step 2	**configure terminal**
	
	Example:
	`Router# configure terminal`
	`Router(config)#`
		Enters global configuration mode.

Step 3	**snmp-server enable traps pppoe**
	
	Example:
	`Router(config)# snmp-server enable traps pppoe`
	`Router(config)#`
		Enables SNMP traps to be sent whenever the number of active sessions exceeds a user-configurable threshold.

Step 4	**exit**
	
	Example:
	`Router(config)# exit`
	`Router#`
		Exits global configuration mode.

Monitoring the PPPoE Termination Feature

To display users who have registered with the Cisco CMTS using PPPoE, use the **show interface cable modem** command:

```
Router# show interface cable 3/0 modem 0

SID    Priv bits  Type      State      IP address     method     MAC address
1      00         host      unknown                   pppoe      00e0.f7a4.5171
1      00         modem     up         10.100.2.35    dhcp       0050.7302.3d81
2      00         modem     up         10.100.2.34    dhcp       0050.7302.3d85

Router#
```

To display the virtual-template interface number being used by a PPPoE client, use the **show vpdn session** command.

```
Router# show vpdn session

L2TP Tunnel and Session Information Total tunnels 1 sessions 1

LocID RemID Remote Name   State  Remote Address  Port  Sessions
34854 14116 R7732-07-ISP1 est    135.1.1.1       1701  1

LocID RemID TunID Intf          Username               State  Last Chg Fastswitch
2     56    34854 Vi1           ppp1@isp1.com          est    00:02:11 enabled

%No active L2F tunnels
%No active PPTP tunnels
PPPoE Tunnel and Session Information Total tunnels 1 sessions 1

PPPoE Tunnel Information
Session count: 1
PPPoE Session Information
SID       RemMAC          LocMAC       Intf     VASt  OIntf         VLAN/
                                                                     VP/VC
1      0050.da80.c13e  0005.00e0.8c8b  Vi1      UP    Ca8/0/1

Router#
```

To display the current VPDN domains, use the **show vpdn domain** command:

```
Router# show vpdn domain

Tunnel          VPDN Group
------          ----------
domain:isp1.com 2 (L2TP)

Router#
```

Configuration Examples for PPPoE Termination

This section lists the following sample configurations for the PPPoE Termination feature:

- PPPoE Configuration for the L2TP Network Server, page 14-24

PPPoE Termination on a Cisco CMTS without L2TP Tunneling

The following configuration configures the Cisco CMTS router to perform PPPoE termination. Traffic from the cable modem users is then sent out over the router's WAN interfaces as IP packets, allowing basic Internet access.

```
version 12.2
!
hostname ubr-pppoe
!
ip cef
no ip domain-lookup
ip domain-name client.com
vpdn enable
no vpdn logging
!
! VPDN group 1 configures the router to accept PPPoE connections and specifies the
! virtual template to be used to configure the virtual interfaces that are created
! for each PPPoE session.
!
vpdn-group 1
 accept-dialin
  protocol pppoe
  virtual-template 1
  pppoe limit per-mac 100
!
! Increase size of small buffers to account for keepalive packets for PPPoE sessions
buffers small permanent 1024
buffers small max-free 1024
buffers small initial 1024
!
interface Ethernet1/0
 ip address 10.100.0.1 255.255.255.0
 ip route-cache flow
 half-duplex
!
! "pppoe enable" command must be configured on each cable interface that is to accept
! PPPoE sessions, but you do not need to configure this command on subinterfaces
interface Cable6/0
 no ip address
 no keepalive
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 589250000
 no cable upstream 0 shutdown
 cable upstream 1 frequency 35008000
 cable upstream 1 power-level 0
 no cable upstream 1 shutdown
 no cable upstream 2 shutdown
 pppoe enable
!
interface Cable6/0.1
 ip address 10.1.1.1 255.255.255.0 secondary
 ip address 10.10.1.1 255.255.255.0
 cable helper-address 10.100.0.100
 no cable proxy-arp
 cable dhcp-giaddr policy
!
```

```
 interface Cable6/0.2
 ip address 10.1.2.1 255.255.255.0 secondary
 ip address 10.10.2.1 255.255.255.0
 cable dhcp-giaddr policy
 cable helper-address 10.100.0.100
!
interface Cable6/0.3
 ip address 10.1.3.1 255.255.255.0
 cable source-verify
 cable dhcp-giaddr policy
 cable helper-address 10.100.0.100
!
! Virtual Template 1 configures the virtual interfaces that will be used
! for PPPoE sessions
interface Virtual-Template1
 ip unnumbered Ethernet1/0
 ip mtu 1492
 ip pim sparse-mode
 peer default ip address pool default
 ppp authentication chap
 no logging event link-status
 no cdp enable
!
```

PPPoE Termination on a Cisco CMTS with L2TP Tunneling

The following configuration configures the Cisco CMTS router to perform PPPoE termination. Traffic received from the cable modem users is sent over the L2TP tunnel to the router that is acting as the L2TP Network Server (LNS).

```
version 12.2
!
hostname ubr-pppoe-l2tp
!
! User name/password sent to LNS to create the L2TP tunnel.
username cmts-user password 0 cmts-password
! User name/password used by LNS to authenticate tunnel creation
username lns-user password 0 lns-password
! User name/password for a PPPoE user - typically this information
! is configured on the RADIUS authentication servers.
username pppoe-user@client.com password 0 user-password
ip cef
no ip domain-lookup
ip domain-name client.com
vpdn enable
no vpdn logging
!
! VPDN group 1 configures the router to accept PPPoE connections and specifies the
! virtual template to be used to configure the virtual interfaces that are created
! for each PPPoE session.
!
vpdn-group 1
 accept-dialin
  protocol pppoe
  virtual-template 1
  pppoe limit per-mac 100
!
! VPDN group 2 configures the group to be used for the L2TP tunnel to the
! LNS (at the IP address of 10.10.15.2) which will be used for PPPoE
! sessions from clients using the domain name as "client.com".
vpdn-group 2
```

```
 request-dialin
  protocol l2tp
  domain client.com
 initiate-to ip 10.10.15.2
local name ubr-pppoe-l2tp
 no l2tp tunnel authentication
!
! Increase size of small buffers to account for keepalive packets for PPPoE sessions
buffers small permanent 1024
buffers small max-free 1024
buffers small initial 1024
!
interface Ethernet1/0
 ip address 10.100.0.1 255.255.255.0
 ip route-cache flow
 half-duplex
!
! "pppoe enable" command must be configured on each cable interface that is to accept
! PPPoE sessions, but you do not need to configure this command on subinterfaces
interface Cable6/0
 no ip address
 no keepalive
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 589250000
 no cable upstream 0 shutdown
 cable upstream 1 frequency 35008000
 cable upstream 1 power-level 0
 no cable upstream 1 shutdown
 no cable upstream 2 shutdown
 pppoe enable
!
interface Cable6/0.1
 ip address 10.1.1.1 255.255.255.0 secondary
 ip address 10.10.1.1 255.255.255.0
 cable helper-address 10.100.0.100
 no cable proxy-arp
 cable dhcp-giaddr policy
!
interface Cable6/0.2
 ip address 10.1.2.1 255.255.255.0 secondary
 ip address 10.10.2.1 255.255.255.0
 cable dhcp-giaddr policy
 cable helper-address 10.100.0.100
!
interface Cable6/0.3
 ip address 10.1.3.1 255.255.255.0
 cable source-verify
 cable dhcp-giaddr policy
 cable helper-address 10.100.0.100
!
! Virtual Template 1 configures the virtual interfaces that will be used
! for PPPoE sessions
interface Virtual-Template1
 ip unnumbered Ethernet1/0
 ip mtu 1492
 ip pim sparse-mode
 peer default ip address pool default
 ppp authentication chap
 no logging event link-status
 no cdp enable
```

PPPoE Client Configuration on a Cisco Router

The following configuration configures a Cisco router that supports PPPoE to act as a PPPoE client. This router connects to the cable modem and performs the PPPoE authentication with the Cisco CMTS that is performing the PPPoE termination.

Note This configuration is for the Cisco 1600 router and needs to be adjusted to fit the interfaces that might be present on other types of routers.

```
!
vpdn enable
no vpdn logging
!
vpdn-group 1
 request-dialin
 protocol pppoe
!
!
interface Ethernet0
 no ip address
 pppoe enable
 pppoe-client dial-pool-number 1
!
interface Dialer1
 mtu 1492
 ip address negotiated
 ip nat outside
 encapsulation ppp
 dialer pool 1
 ppp chap hostname joeuser@client.com
 ppp chap password 7 12139CA0C041104
!
ip nat inside source list 1 interface Dialer1 overload

ip route 0.0.0.0 0.0.0.0 Dialer1
!
access-list 1 permit any
```

PPPoE Configuration for the L2TP Network Server

The following sample configuration shows a Cisco router being configured to act as the L2TP Network Server (LNS). This router terminates the L2TP tunnel from the Cisco CMTS and forwards the traffic from the PPPoE sessions to the corporate network.

```
!
hostname lns-router
!
! User name/password for the LNS itself
username lns-user password 0 lns-password
! User name/password for the Cisco CMTS
username cmts-user password 0 cmts-password
! Username and password for the PPPoE client - typically this information is
! configured on the RADIUS authentication servers
username pppoe-user@client.com password 0 user-password
!
ip subnet-zero
ip cef
ip domain-name client.com
```

```
!
vpdn enable
no vpdn logging
!
vpdn-group 1
 accept-dialin
  protocol l2tp
  virtual-template 1
 terminate-from hostname ubr-pppoe-l2tp
 no l2tp tunnel authentication
!
! Allows the LNS to preconfigure virtual templates
! for the PPPoE sessions, allowing the sessions to come up faster
virtual-template 1 pre-clone 2000
!
interface loopback 0
ip address 9.10.7.1 255.255.255.0
!
!
interface Virtual-Template1
 ip unnumbered loopback 0
 ip mroute-cache
 ip mtu 1492
 peer default ip address pool pool-1 pool-2
!
ip local pool pool-1 9.10.7.3 9.10.7.254
ip local pool pool-2 9.10.8.1 9.10.8.254
```

Additional References

For additional information related to configuring PPPoE Termination on the Cisco CMTS, refer to the following references:

Related Documents

Related Topic	Document Title
Configuring PPP over Ethernet	Configuring Broadband Access: PPP and Routed Bridge Encapsulation, Cisco IOS Wide-Area Networking Configuration Guide, Release 12.2, at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fwan_c/wcfppp.htm
Enabling SNMP Traps for PPPoE Active Sessions	*PPPoE Session-Count MIB* **Note** This document has reached End of Life. For more information, see the following End-of-Life Announcement at the following URL: http://www.cisco.com/en/US/docs/ios/redirect/eol.html
Configuring Virtual Private Networks (VPNs)	Configuring Virtual Private Networks, Cisco IOS Dial Service Configuration Guide: Network Services, Release 12.1 **Note** This document has reached End of Life. For more information, see the following End-of-Life Announcement at the following URL: http://www.cisco.com/en/US/docs/ios/redirect/eol.html
CMTS Command Reference	*Cisco Broadband Cable Command Reference Guide,* at the following URL: http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html
Cisco IOS Release 12.2 Command Reference	Cisco IOS Release 12.2 Configuration Guides and Command References, at the following URL: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_installation_and_configuration_guides_list.html http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html

Standards

Standards[1]	Title
SP-RFIv1.1-I08-020301	Data-Over-Cable Service Interface Specifications Radio Frequency Interface Specification, version 1.1 (http://www.cablelabs.com/cablemodem)

1. Not all supported standards are listed.

MIBs

MIBs[1]	MIBs Link
CISCO-PPPOE-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

1. Not all supported MIBs are listed.

RFCs

RFCs[1]	Title
RFC 1483	Multiprotocol Encapsulation over ATM Adaptation Layer 5
RFC 2516	A Method for Transmitting PPP Over Ethernet (PPPoE)
RFC 2865	Remote Authentication Dial In User Service (RADIUS)
RFC 2866	RADIUS Accounting

1. Not all supported RFCs are listed.

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/cisco/web/support/index.html