



VPDN Tunnel Management

First Published: September 30, 2007

Last Updated: November 20, 2009

This module contains information about managing virtual private dialup network (VPDN) tunnels and monitoring VPDN events. The tasks documented in this module should be performed only after configuring and deploying a VPDN.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for VPDN Tunnel Management”](#) section on page 32.

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for VPDN Tunnel Management, page 2](#)
- [Information About VPDN Tunnel Management, page 2](#)
- [How to Manage VPDN Tunnels, page 4](#)
- [Configuration Examples for VPDN Tunnel Management, page 26](#)
- [Additional References, page 30](#)
- [Feature Information for VPDN Tunnel Management, page 32](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Prerequisites for VPDN Tunnel Management

Before you can perform the tasks in this module, you must configure a VPDN deployment. For an overview of VPDN deployments, refer to the “[VPDN Technology Overview](#)” module.

Information About VPDN Tunnel Management

Before you perform the tasks in this module, you should understand the following concepts:

- [Termination of VPDN Tunnels, page 2](#)
- [VPDN Session Limits, page 2](#)
- [Control Packet Parameters for VPDN Tunnels, page 3](#)
- [L2TP Congestion Avoidance, page 3](#)
- [VPDN Extended Failover, page 3](#)
- [VPDN Event Logging, page 4](#)

Termination of VPDN Tunnels

VPDN tunnels can be terminated manually or through a soft shutdown. Manual termination of a VPDN tunnel results in the immediate shut down of the specified VPDN tunnel and all sessions within that tunnel, resulting in a sudden disruption of VPDN services. Enabling soft shutdown on a router prevents the establishment of new VPDN sessions in all VPDN tunnels that terminate on that router, but does not affect existing sessions. Opting to terminate a VPDN tunnel by enabling soft shutdown prevents the disruption of established sessions that occurs when a VPDN tunnel is manually terminated.

VPDN Session Limits

The number of simultaneous VPDN sessions that can be established on a router can be manually configured, providing network administrators more control over the network. VPDN session limits can increase performance and reduce latency for routers that are otherwise forced to operate at high capacity.

The maximum number of VPDN sessions can be configured globally, at the level of a VPDN group, or for all VPDN groups associated with a particular VPDN template.

The hierarchy for the application of VPDN session limits is as follows:

- Globally configured session limits take precedence over session limits configured for a VPDN group or in a VPDN template. The total number of sessions on a router may not exceed a configured global session limit.
- Session limits configured for a VPDN template are enforced for all VPDN groups associated with that VPDN template. The total number of sessions for all of the associated VPDN groups may not exceed the configured VPDN template session limit.
- Session limits configured for a VPDN group are enforced for that VPDN group.

Control Packet Parameters for VPDN Tunnels

Certain control packet timers, retry counters, and the advertised control packet receive window size can be configured for Layer 2 Transport Protocol (L2TP) or Layer 2 Forwarding (L2F) VPDN tunnels. Adjustments to these parameters allow fine-tuning of router performance to suit the particular needs of the VPDN deployment.

L2TP Congestion Avoidance

L2TP congestion avoidance provides packet flow control and congestion avoidance by throttling L2TP control messages as described in RFC 2661. Throttling L2TP control message packets prevents input buffer overflows on the peer tunnel endpoint, which can result in dropped sessions.

Before the introduction of L2TP congestion avoidance, the window size used to send packets between the network access server (NAS) and the tunnel server was set to the value advertised by the peer endpoint and was never changed. Configuring L2TP congestion avoidance allows the L2TP packet window to be dynamically resized using a sliding window mechanism. The window size grows larger when packets are delivered successfully, and is reduced when dropped packets must be retransmitted.

L2TP congestion avoidance is useful in networks with a relatively high rate of calls being placed by either tunnel endpoint. L2TP congestion avoidance is also useful on highly scalable platforms such as the Cisco 10000 router, which supports a large number of simultaneous sessions.

VPDN Extended Failover

Before Cisco IOS Release 12.2(13)T, L2TP failover described only one scenario: During tunnel establishment, if a router sent a Start-Control-Connection-Request (SCCRQ) message a number of times and received no response from the peer, the router could then “fail over” to the IP address of another peer (if so configured) and attempt tunnel establishment with that peer.

Cisco IOS Release 12.2(13)T, extended L2TP failover to accommodate the following two scenarios:

- During tunnel establishment, a router receives a StopCCN message from its peer.
- During session establishment, a router receives a CDN message from its peer.

In either case, the router marks the peer IP address as busy for a period of time (60 seconds) during which no attempt to establish a session or tunnel will be made to that peer. The router then selects an alternate peer to contact. If a tunnel is already established to this alternate peer, the router uses the existing tunnel to bring up the new session. Otherwise, the router will send an SCCRQ message to the alternate peer to initiate tunnel establishment.

Beginning with Cisco IOS Release 12.2(31)ZV, the VPDN Extended Failover feature extends the Result Code and Error Code values to include all L2TP CDN result codes, generating a failover if the L2TP session is not established.

The following L2TP CDN result codes are exceptions for failover because they are considered session-specific errors:

- L2TP_RESULT_CDN_CARRIER_LOSS(1)
- L2TP_RESULT_CDN_NO_CARRIER(7)
- L2TP_RESULT_CDN__BUSY(8)
- L2TP_RESULT_CDN_NO_DIAL_TONE(9)
- L2TP_RESULT_CDN_TIMEOUT(10)
- L2TP_RESULT_CDN_BAD_FRAMING(11)

How VPDN Extended Failover Works

The VPDN Extended Failover feature extends L2TP failover to occur if during tunnel establishment an LN) receives a StopCCN message from its peer or during session establishment an LNS receives a CDN message from its peer. In either case, the LNS selects an alternate peer to contact.

A Result Code attribute-value pair (AVP) is included in both the StopCCN and CDN control messages that indicates the reason for tunnel or session termination, respectively. This AVP may also include an optional Error Code, which further describes the nature of the termination. The various Result Code and Error Code values were standardized in RFC 2661.

Failover Through an LTS

The VPDN Extended Failover feature provides support for failover when using an L2TP Tunnel Switch (LTS) by using the following error code:

L2TP_VENDOR_ERROR_GROUP_BUSY(6)

This error indicates that all of the IP addresses specified in the VPDN group are busy.

In addition, the IP address of the LNS or LTS is placed on the busy list, even when an L2TP session is established, when the following CDN messages are received:

L2TP_RESULT_CDN_ERROR
L2TP_ERROR_VENDOR_SPECIFIC
L2TP_ERROR_VENDOR_GROUP_BUSY
L2TP_ERROR_VENDOR_SLIMIT

VPDN Event Logging

There are two types of VPDN event logging available, VPDN failure event logging and generic VPDN event logging. The logging of VPDN failure events is enabled by default. Generic VPDN event logging is disabled by default, and must be explicitly enabled before generic event messages can be viewed.

How to Manage VPDN Tunnels

Perform any of the following tasks to manage your VPDN tunnels:

- [Manually Terminating VPDN Tunnels, page 5](#) (optional)
- [Enabling Soft Shutdown of VPDN Tunnels, page 6](#) (optional)
- [Verifying the Soft Shutdown of VPDN Tunnels, page 7](#) (optional)
- [Limiting the Number of Allowed Simultaneous VPDN Sessions, page 9](#) (optional)
- [Verifying VPDN Session Limits, page 12](#) (optional)
- [Configuring L2TP Control Packet Parameters for VPDN Tunnels, page 13](#) (optional)
- [Configuring L2F Control Packet Parameters for VPDN Tunnels, page 17](#) (optional)
- [Configuring L2TP Congestion Avoidance, page 19](#) (optional)
- [Configuring VPDN Failure Event Logging, page 24](#) (optional)
- [Enabling Generic VPDN Event Logging, page 25](#) (optional)

Manually Terminating VPDN Tunnels

Manual termination of a VPDN tunnel results in the immediate shutdown of the specified VPDN tunnel and all sessions within that tunnel, resulting in a sudden disruption of VPDN services. Before manually terminating a VPDN tunnel, you may want to consider performing the task in the “[Enabling Soft Shutdown of VPDN Tunnels](#)” section instead.

A manually terminated VPDN tunnel can be restarted immediately when a user logs in. Manually terminating and restarting a VPDN tunnel while VPDN event logging is enabled can provide useful troubleshooting information about VPDN session establishment.

Perform this task to manually shut down a specific VPDN tunnel, resulting in the termination of the tunnel and all sessions in that tunnel. You may perform this task on the following devices:

- The tunnel server
- The NAS when it is functioning as a tunnel endpoint

Restrictions

For Point-to-Point Tunneling Protocol (PPTP) tunnels and client-initiated L2TP tunnels, you may perform this task only on the tunnel server.

SUMMARY STEPS

1. **enable**
2. **clear vpdn tunnel** [**pptp** | **l2f** | **l2tp**] [**all** | **hostname** *remote-host-name* [*local-name*] | **id** *local-tunnel-id* | **ip local** *ip-address* | **ip remote** *ip-address*]
- 3.
4. **clear vpdn tunnel** {**pptp** | **l2tp**} {**all** | **hostname** *remote-name* [*local-name*] | **id** *local-id* | **ip** *local-ip-address* | **ip** *remote-ip-address*}
or
clear vpdn tunnel l2f {**all** | **hostname** *nas-name* *hgw-name* | **id** *local-id* | **ip** *local-ip-address* | **ip** *remote-ip-address*}

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example: Router> enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<p>clear vpdn tunnel {pptp l2tp} {all hostname remote-name [local-name] id local-id ip local-ip-address ip remote-ip-address}</p> <p>OR</p> <p>clear vpdn tunnel l2f {all hostname nas-name hgw-name id local-id ip local-ip-address ip remote-ip-address}</p> <p>Example: Router# clear vpdn tunnel l2tp all</p> <p>OR</p> <p>Router# clear vpdn tunnel l2f hostname nas12 hgw32</p>	<p>Shuts down a specified tunnel and all sessions within the tunnel.</p>

What to Do Next

If you would like to observe VPDN tunnel event messages during the reestablishment of the cleared tunnel, you may perform the task in the “[Enabling Generic VPDN Event Logging](#)” section.

Enabling Soft Shutdown of VPDN Tunnels

Enabling soft shutdown of VPDN tunnels on a router prevents the establishment of new VPDN sessions in all VPDN tunnels that terminate on that router, but does not affect existing sessions. Opting to terminate a VPDN tunnel by enabling soft shutdown prevents the disruption of established sessions that occurs when a VPDN tunnel is manually terminated. Enabling soft shutdown on a router or access server will affect all of the tunnels terminating on that device. There is no way to enable soft shutdown for a specific tunnel. If you want to shut down a specific tunnel on a device without affecting any other tunnels, you may perform the task in the “[Manually Terminating VPDN Tunnels](#)” section instead.

When soft shutdown is performed on a NAS, the potential session will be authorized before it is refused. This authorization ensures that accurate accounting records can be kept.

When soft shutdown is performed on a tunnel server, the reason for the session refusal will be returned to the NAS. This information is recorded in the VPDN history failure table.

**Note**

Enabling soft shutdown of VPDN tunnels does not affect the establishment of Multichassis Multilink PPP (MMP) tunnels.

Perform this task to prevent new sessions from being established in any VPDN tunnel terminating on the router without disturbing service for existing sessions. You may perform this task on the following devices:

- The tunnel server
- The NAS when it is functioning as a tunnel endpoint

Restrictions

- For PPTP tunnels and client-initiated L2TP tunnels, you may perform this task only on the tunnel server.
- Enabling soft shutdown of VPDN tunnels will not prevent new MMP sessions from being established.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn softshut**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	vpdn softshut Example: Router(config)# vpdn softshut	Prevents new sessions from being established on a VPDN tunnel without disturbing existing sessions.

What to Do Next

You may proceed to the optional task in the “[Verifying the Soft Shutdown of VPDN Tunnels](#)” section.

Verifying the Soft Shutdown of VPDN Tunnels

Perform this task to ensure that soft shutdown is working properly.

SUMMARY STEPS

1. Establish a VPDN session by dialing in to the NAS using an allowed username and password.

2. **enable**
3. **configure terminal**
4. **vpdn softshut**
5. **exit**
6. **show vpdn**
7. Attempt to establish a new VPDN session by dialing in to the NAS using a second allowed username and password.
8. show vpdn history failure

DETAILED STEPS

Step 1 Establish a VPDN session by dialing in to the NAS using an allowed username and password.

Step 2 **enable**

Enter this command to enable privileged EXEC mode. Enter your password if prompted:

```
Router> enable
```

Step 3 **configure terminal**

Enters global configuration mode.

```
Router# configure terminal
```

Step 4 **vpdn softshut**

Prevents new sessions from being established on a VPN tunnel without disturbing existing sessions. You may issue this command on either the NAS or the tunnel server.

```
Router(config)# vpdn softshut
```

Step 5 **exit**

Exits to privileged EXEC mode.

```
Router(config)# exit
```

Step 6 **show vpdn**

Displays information about active L2TP or L2F tunnels and message identifiers in a VPDN. Issue this command to verify that the original session is active:

```
Router# show vpdn
```

```
% No active L2TP tunnels
```

```
L2F Tunnel and Session
```

NAS	CLID	HGW	CLID	NAS Name	HGW Name	State
36		1		NAS1	tunnelserver1	open
				172.25.52.8	172.25.52.7	

CLID	MID	Username	Intf	State
36	1	user1@cisco.com	Vi1	open

Step 7 Attempt to establish a new VPDN session by dialing in to the NAS using a second allowed username and password.

If soft shutdown has been enabled, a system logging (syslog) message similar to the following should appear on the console of the soft shutdown router:

```
00:11:17:%VPDN-6-SOFTSHUT:L2F HGW tunnelserver1 has turned on softshut and rejected user user2@cisco.com
```

Step 8 show vpdn history failure

Shows the content of the history failure table.

```
Router# show vpdn history failure
```

```
User:user2@ cisco.com
NAS:NAS1, IP address = 172.25.52.8, CLID = 2
Gateway:tunnelserver1, IP address = 172.25.52.7, CLID = 13
Log time:00:04:21, Error repeat count:1
!
!This output demonstrates that soft shutdown has been successful.
Failure type:VPDN softshut has been activated.
!
Failure reason:
```

Limiting the Number of Allowed Simultaneous VPDN Sessions

The number of simultaneous VPDN sessions that can be established on a router can be manually configured, providing network administrators more control over the network. VPDN session limits can increase performance and reduce latency for routers that are otherwise forced to operate at high capacity.

The maximum number of VPDN sessions can be configured globally, at the level of a VPDN group, or for all VPDN groups associated with a particular VPDN template.

The hierarchy for the application of VPDN session limits is as follows:

- Globally configured session limits take precedence over session limits configured for a VPDN group or in a VPDN template. The total number of sessions on a router may not exceed a configured global session limit.
- Session limits configured for a VPDN template are enforced for all VPDN groups associated with that VPDN template. The total number of sessions for all of the associated VPDN groups may not exceed the configured VPDN template session limit.
- Session limits configured for a VPDN group are enforced for that VPDN group.

For an example of the interactions of global, template-level, and group-level VPDN session limits, see the [“Configuring VPDN Session Limits: Examples”](#) section.

Perform any or all of the following optional tasks to configure VPDN session limits:

- [Configuring Global VPDN Session Limits, page 10](#) (optional)
- [Configuring VPDN Session Limits in a VPDN Template, page 10](#) (optional)
- [Configuring Session Limits for a VPDN Group, page 11](#) (optional)

You may perform these tasks on the NAS or the tunnel server.

Restrictions

For PPTP tunnels and client-initiated L2TP tunnels, you may perform these tasks only on the tunnel server.

Configuring Global VPDN Session Limits

Perform this task to limit the total number of VPDN sessions allowed on the router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn session-limit *sessions***

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	vpdn session-limit <i>sessions</i> Example: Router(config)# vpdn session-limit 6	Limits the number of simultaneous VPDN sessions globally on the router.

What to Do Next

- You may perform the optional task in the “[Configuring VPDN Session Limits in a VPDN Template](#)” section.
- You may perform the optional task in the “[Configuring Session Limits for a VPDN Group](#)” section.
- You may perform the optional task in the “[Verifying VPDN Session Limits](#)” section.

Configuring VPDN Session Limits in a VPDN Template

Perform this task to configure a session limit in a VPDN template. The session limit will be applied across all VPDN groups associated with the VPDN template.

Prerequisites

- You must be running Cisco IOS Release 12.2(13)T or a later release.
- A VPDN template must be configured. To configure a VPDN template, perform the task “[Creating a VPDN Template](#)” in the “[Configuring Additional VPDN Features](#)” module.
- If you configure a named VPDN template, you must associate the desired VPDN groups with the VPDN template. To associate a VPDN group with a VPDN template, perform the task “[Associating a VPDN Group with a VPDN Template](#)” in the “[Configuring Additional VPDN Features](#)” module.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn-template** *[name]*
4. **group session-limit** *sessions*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	vpdn-template <i>[name]</i> Example: Router(config)# vpdn-template l2tp	Creates a VPDN template and enters VPDN template configuration mode.
Step 4	group session-limit <i>sessions</i> Example: Router(config-vpdn-templ)# group session-limit 6	Specifies the maximum concurrent sessions allowed across all VPDN groups associated with a particular VPDN template.

What to Do Next

- You may perform the optional task in the “[Configuring Session Limits for a VPDN Group](#)” section.
- You may perform the optional task in the “[Verifying VPDN Session Limits](#)” section.

Configuring Session Limits for a VPDN Group

Perform this task to limit the number of VPDN sessions at the VPDN group level.

Prerequisites

You must be running Cisco IOS Release 12.2(4)T, Cisco IOS Release 12.2(28)SB, or a later release.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn-group** *name*
4. **session-limit** *number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	vpdn-group <i>name</i> Example: Router(config)# vpdn group 1	Associates a VPDN group to a customer or VPDN profile and enters VPDN group configuration mode.
Step 4	session-limit <i>number</i> Example: Router(config-vpdn)# session-limit 2	Limits the number of sessions that are allowed through a specified VPDN group.

What to Do Next

You may perform the optional task in the “[Verifying VPDN Session Limits](#)” section.

Verifying VPDN Session Limits

Perform this task to ensure that VPDN sessions are being limited properly.



Note

If you use a Telnet session to connect to the NAS, enable the **terminal monitor** command, which ensures that your EXEC session is receiving the logging and debug output from the NAS.

SUMMARY STEPS

- enable**
- configure terminal**
- vpdn session-limit** *sessions*
- Establish a VPDN session by dialing in to the NAS using an allowed username and password.
- Attempt to establish a new VPDN session by dialing in to the NAS using a second allowed username and password.
- exit**
- show vpdn history failure**

DETAILED STEPS

Step 1 enable

Enter this command to enable privileged EXEC mode. Enter your password if prompted:

```
Router> enable
```

Step 2 configure terminal

Enters global configuration mode.

```
Router# configure terminal
```

Step 3 vpdn session-limit sessions

Limits the number of simultaneous VPDN sessions on the router to the number specified with the *sessions* argument.

Issue this command on either the NAS or the tunnel server.

```
Router(config)# vpdn session-limit 1
```

Step 4 Establish a VPDN session by dialing in to the NAS using an allowed username and password.**Step 5** Attempt to establish a new VPDN session by dialing in to the NAS using a second allowed username and password.

If VPDN session limits have been configured properly, this session will be refused and a syslog message similar to the following should appear on the console of the router:

```
00:11:17:%VPDN-6-MAX_SESS_EXCD:L2F HGW tunnelserver1 has exceeded configured local session-limit and rejected user user2@cisco.com
```

Step 6 exit

Exits to privileged EXEC mode.

Step 7 show vpdn history failure

Shows the content of the history failure table.

```
Router# show vpdn history failure
```

```
User:user2@cisco.com
NAS:NAS1, IP address = 172.25.52.8, CLID = 2
Gateway:tunnelserver1, IP address = 172.25.52.7, CLID = 13
Log time:00:04:21, Error repeat count:1
Failure type:Exceeded configured VPDN maximum session limit.
!This output shows that the configured session limit is being properly applied.
Failure reason:
```

Configuring L2TP Control Packet Parameters for VPDN Tunnels

Control packet timers, retry counters, and the advertised control packet receive window size can be configured for L2TP VPDN tunnels. Adjustments to these parameters allow fine-tuning of router performance to suit the particular needs of the VPDN deployment.

Perform this task to configure control packet parameters if your VPDN configuration uses L2TP tunnels. The configuration of each parameter is optional. If a parameter is not manually configured, the default value will be used.

You may perform this task on the following devices:

- The tunnel server
- The NAS when it is functioning as a tunnel endpoint

Prerequisites

- You must be running Cisco IOS Release 12.2(4)T, Cisco IOS Release 12.2(28)SB, or a later release to configure the **l2tp tunnel retransmit initial timeout**, **l2tp tunnel retransmit initial retries**, or **l2tp tunnel busy timeout** command.
- Load balancing must be enabled for the configuration of the **l2tp tunnel retransmit initial timeout** command or the **l2tp tunnel retransmit initial retries** command to have any effect.

Restrictions

For client-initiated L2TP tunnels, you may perform this task only on the tunnel server.

SUMMARY STEPS

1. enable
2. **configure terminal**
3. **vpdn-group** *name*
4. **l2tp tunnel hello** *seconds*
5. **l2tp tunnel receive window** *packets*
6. **l2tp tunnel retransmit retries** *number*
7. **l2tp tunnel retransmit timeout** {*min* | *max*} *seconds*
8. **l2tp tunnel timeout no-session** {*seconds* | **never**}
9. **l2tp tunnel timeout setup** *seconds*
10. **l2tp tunnel zlb delay** *seconds*
11. **l2tp tunnel retransmit initial timeout** {*min* | *max*} *time*
12. **l2tp tunnel retransmit initial retries** *number*
13. **l2tp tunnel busy timeout** *seconds*

DETAILED STEPS2

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example: Router> enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example: Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p>vpdn-group name</p> <p>Example: Router(config)# vpdn-group group1</p>	<p>Associates a VPDN group to a customer or VPDN profile and enters VPDN group configuration mode.</p>
Step 4	<p>l2tp tunnel hello seconds</p> <p>Example: Router(config-vpdn)# l2tp tunnel hello 90</p>	<p>(Optional) Set the number of seconds between sending hello keepalive packets for an L2TP tunnel.</p> <ul style="list-style-type: none"> <i>seconds</i>—Interval, in seconds, that the NAS and tunnel server wait before sending the next L2TP tunnel keepalive packet. Valid values range from 0 to 1000. The default value is 60.
Step 5	<p>l2tp tunnel receive window packets</p> <p>Example: Router(config-vpdn)# l2tp tunnel receive window 500</p>	<p>(Optional) Configures the number of packets allowed in the local receive window for an L2TP control channel.</p> <ul style="list-style-type: none"> <i>packets</i>—Number of packets allowed in the receive window. Valid values range from 1 to 5000. The default value varies by platform.
Step 6	<p>l2tp tunnel retransmit retries number</p> <p>Example: Router(config-vpdn)# l2tp tunnel retransmit retries 8</p>	<p>(Optional) Configures the number of retransmission attempts made for an L2TP control packet.</p> <ul style="list-style-type: none"> <i>number</i>—Number of retransmission attempts. Valid values range from 5 to 1000. The default value is 10.
Step 7	<p>l2tp tunnel retransmit timeout {min max} seconds</p> <p>Example: Router(config-vpdn)# l2tp tunnel retransmit timeout max 4</p>	<p>(Optional) Configures the amount of time that the router will wait before resending an L2TP control packet.</p> <ul style="list-style-type: none"> min—Specifies the minimum time that the router will wait before resending a control packet. max—Specifies the maximum time that the router will wait before resending a control packet. <i>seconds</i>—Timeout length, in seconds, the router will wait before resending a control packet. Valid values range from 1 to 8. The default minimum value is 1. The default maximum value is 8.

	Command or Action	Purpose
Step 8	<p>12tp tunnel timeout no-session {<i>seconds</i> <i>never</i>}</p> <p>Example: Router(config-vpdn)# 12tp tunnel timeout no-session never</p>	<p>(Optional) Configures the time a router waits after an L2TP tunnel becomes empty before tearing down the tunnel.</p> <ul style="list-style-type: none"> <i>seconds</i>—Time, in seconds, the router waits before tearing down an empty L2TP tunnel. Valid values range from 0 to 86400. If the router is configured as a NAS, the default is 15 seconds. If the router is configured as a tunnel server, the default is 10. never—Specifies that the router will never tear down an empty L2TP tunnel.
Step 9	<p>12tp tunnel timeout setup <i>seconds</i></p> <p>Example: Router(config-vpdn)# 12tp tunnel timeout setup 25</p>	<p>(Optional) Configures the amount of time that the router will wait for a confirmation message after sending out the initial L2TP control packet before considering a peer busy.</p> <ul style="list-style-type: none"> <i>seconds</i>—Time, in seconds, the router will wait for a confirmation message. Valid values range from 60 to 6000. The default value is 10.
Step 10	<p>12tp tunnel zlb delay <i>seconds</i></p> <p>Example: Router(config-vpdn)# 12tp tunnel zlb delay 2</p>	<p>(Optional) Configures the delay time before a zero length bit (ZLB) control message must be acknowledged.</p> <ul style="list-style-type: none"> <i>seconds</i>—Maximum number of seconds the router will delay before acknowledging ZLB control messages. Valid values range from 1 to 5. The default value is 3.
Step 11	<p>12tp tunnel retransmit initial timeout {<i>min</i> <i>max</i>} <i>time</i></p> <p>Example: Router(config-vpdn)# 12tp tunnel retransmit initial timeout min 2</p>	<p>(Optional—Cisco IOS Release 12.2(4)T, Cisco IOS Release 12.2(28)SB, or a later release) Sets the amount of time, in seconds, that the router will wait before resending an initial packet out to establish a tunnel.</p> <ul style="list-style-type: none"> min—Specifies the minimum time that the router will wait before resending an initial packet. max—Specifies the maximum time that the router will wait before resending an initial packet. <i>seconds</i>—Timeout length, in seconds, the router will wait before resending an initial packet. Valid values range from 1 to 8. The default minimum value is 1. The default maximum value is 8. <p>Note Load balancing must be configured for the retry counter configured with the 12tp tunnel retransmit initial timeout command to take effect.</p>

Command or Action	Purpose
<p>Step 12 <code>l2tp tunnel retransmit initial retries number</code></p> <p>Example: <pre>Router(config-vpdn)#l2tp tunnel retransmit initial retries 5</pre></p>	<p>(Optional—Cisco IOS Release 12.2(4)T, Cisco IOS Release 12.2(28)SB, or a later release) Sets the number of times that the router will attempt to send out the initial control packet for tunnel establishment before considering a router busy.</p> <ul style="list-style-type: none"> <i>number</i>—Number of retransmission attempts. Valid values range from 1 to 1000. The default value is 2. <p>Note Load balancing must be configured for the retry counter configured with the l2tp tunnel retransmit initial retries command to take effect.</p>
<p>Step 13 <code>l2tp tunnel busy timeout seconds</code></p> <p>Example: <pre>Router(config-vpdn)#l2tp tunnel busy timeout 90</pre></p>	<p>(Optional—Cisco IOS Release 12.2(4)T, Cisco IOS Release 12.2(28)SB, or a later release) Configures the amount of time, in seconds, that the router will wait before attempting to recontact a router that was previously busy.</p> <ul style="list-style-type: none"> <i>seconds</i>—Time, in seconds, to wait before checking for router availability. Valid values range from 60 to 6000. The default value is 300.

Configuring L2F Control Packet Parameters for VPDN Tunnels

Beginning in Cisco IOS Release 12.2(4)T and Cisco IOS Release 12.2(28)SB, certain control packet timers and retry counters can be configured for L2F VPDN tunnels. Adjustments to these parameters allow fine-tuning of router performance to suit the particular needs of the VPDN deployment.

Perform this task to configure control packet timers and retry counters if your VPDN configuration uses L2F tunnels. The configuration of each parameter is optional. If a parameter is not manually configured, the default values will be used.

You may perform this task on the NAS or the tunnel server.

Prerequisites

You must be running Cisco IOS Release 12.2(4)T, Cisco IOS Release 12.2(28)SB, or a later release.

Restrictions

Load balancing must be enabled for the configuration of the **l2f tunnel retransmit initial retries** command to have any effect.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn-group name**
4. **l2f tunnel timeout setup seconds**
5. **l2f tunnel retransmit initial retries number**

6. **l2f tunnel busy timeout** *seconds*
7. **l2f tunnel retransmit retries** *number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example: Router> enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example: Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p>vpdn-group name</p> <p>Example: Router(config)# vpdn-group group1</p>	<p>Associates a VPDN group to a customer or VPDN profile and enters VPDN group configuration mode.</p>
Step 4	<p>l2f tunnel timeout setup seconds</p> <p>Example: Router(config-vpdn)# l2f tunnel timeout setup 25</p>	<p>(Optional) Sets the amount of time that the router will wait for a confirmation message after sending out the initial control packet before considering a router busy.</p> <ul style="list-style-type: none"> <i>seconds</i>—Time, in seconds, the router will wait for a return message. Valid values range from 60 to 6000. The default value is 10.
Step 5	<p>l2f tunnel retransmit initial retries number</p> <p>Example: Router(config-vpdn)# l2f tunnel retransmit initial retries 5</p>	<p>(Optional) Sets the number of times that the router will attempt to send the initial control packet for tunnel establishment before considering a router busy.</p> <ul style="list-style-type: none"> <i>number</i>—Number of retries that will be attempted. Valid values range from 1 to 1000. The default value is 2. <p>Note Load balancing must be configured for the retry counter configured with the l2f tunnel retransmit initial retries command to take effect.</p>
Step 6	<p>l2f tunnel busy timeout seconds</p> <p>Example: Router(config-vpdn)# l2f tunnel busy timeout 90</p>	<p>(Optional) Configures the amount of time that the router will wait before attempting to recontact a router that was previously busy.</p> <ul style="list-style-type: none"> <i>seconds</i>—Time, in seconds, to wait before checking for peer availability. Valid values range from 60 to 6000. The default value is 300.
Step 7	<p>l2f tunnel retransmit retries number</p> <p>Example: Router(config-vpdn)# l2f tunnel retransmit retries 10</p>	<p>(Optional) Sets the number of times the router will attempt to resend tunnel control packets before tearing the tunnel down.</p>

Configuring L2TP Congestion Avoidance

L2TP congestion avoidance provides packet flow control and congestion avoidance by throttling L2TP control messages as described in RFC 2661. Throttling L2TP control message packets prevents input

buffer overflows on the peer tunnel endpoint, which can result in dropped sessions.

Before the introduction of L2TP congestion avoidance, the window size used to send packets between the NAS and the tunnel server was set to the value advertised by the peer endpoint and was never changed. Configuring L2TP congestion avoidance allows the L2TP packet window to be dynamically resized using a sliding window mechanism. The window size grows larger when packets are delivered successfully, and is reduced when dropped packets must be retransmitted.

L2TP congestion avoidance is useful in networks with a relatively high rate of calls being placed by either tunnel endpoint. L2TP congestion avoidance is also useful on highly scalable platforms such as the Cisco 10000 router, which supports a large number of simultaneous sessions.

The following sections contain additional information about L2TP congestion avoidance:

- [How L2TP Congestion Avoidance Works, page 20](#)
- [Prerequisites for L2TP Congestion Avoidance, page 21](#)
- [Restrictions for L2TP Congestion Avoidance, page 21](#)

Perform the following tasks to configure L2TP congestion avoidance:

- [Enabling L2TP Congestion Avoidance on the Sending Device, page 21](#) (required)
- [Verifying L2TP Congestion Avoidance, page 22](#) (optional)

How L2TP Congestion Avoidance Works

TCP/IP and RFC 2661 define two algorithms—slow start and congestion avoidance—used to throttle control message traffic between a NAS and a tunnel server. Slow start and congestion avoidance are two independent algorithms that work together to control congestion. Slow start and congestion avoidance require that two variables, a slow start threshold (SSTHRESH) size and a congestion window (CWND) size, be maintained by the sending device for each connection.

The congestion window defines the number of packets that can be transmitted before the sender must wait for an acknowledgment from its peer. The size of the congestion window expands and contracts, but may never exceed the size of the peer device's advertised receive window.

The slow start threshold defines the point at which the sending device switches operation from slow start mode to congestion avoidance mode. When the congestion window size is smaller than the slow start threshold, the device operates in slow start mode. When the congestion window size equals the slow start threshold, the device switches to congestion avoidance mode.

When a new connection is established, the sending device initially operates in slow start mode. The congestion window size is initialized to one packet, and the slow start threshold is set to the receive window size advertised by the peer tunnel endpoint (the receiving side).

The sending device begins by transmitting one packet and waiting for it to be acknowledged. When the acknowledgment is received, the congestion window size is incremented from one to two, and two packets can be sent. When those two packets are each acknowledged, the congestion window is increased to four. The congestion window doubles for each complete round trip, resulting in an exponential increase in size.

When the congestion window size reaches the slow start threshold value, the sending device switches over to operate in congestion avoidance mode. Congestion avoidance mode slows down the rate at which the congestion window size grows. In congestion avoidance mode, for every acknowledgment received the congestion window increases at the rate of 1 divided by the congestion window size. This results in linear, rather than exponential, growth of the congestion window size.

At some point, the capacity of the peer device will be exceeded and packets will be dropped. This indicates to the sending device that the congestion window has grown too large. When a retransmission event is detected, the slow start threshold value is reset to half of the current congestion window size, the congestion window size is reset to one, and the device switches operation to slow start mode (if it was not already operating in that mode).

Prerequisites for L2TP Congestion Avoidance

You must be running Cisco IOS Release 12.2(28)SB or a later release.

Restrictions for L2TP Congestion Avoidance

- This task is compatible only with VPDN deployments that use the L2TP tunneling protocol.
- For client-initiated L2TP tunnels, you may perform this task only on the tunnel server.
- The congestion window size may not exceed the size of the advertised receive window set by the **l2tp tunnel receive-window** command on the peer device. You may perform the task in the “[Configuring L2TP Control Packet Parameters for VPDN Tunnels](#)” section on the remote peer device to configure the advertised receive window.
- L2TP congestion avoidance is enabled (or disabled) only for those tunnels that are established after the configuration has been applied. Tunnels that already exist when the **l2tp congestion-control** command is issued are not affected by the command.

Enabling L2TP Congestion Avoidance on the Sending Device

Perform this task to enable L2TP congestion avoidance on a tunnel endpoint, allowing dynamic throttling of the L2TP control packet window size.

You may perform this task on the following devices:

- The tunnel server
- The NAS when it is functioning as a tunnel endpoint

This task need only be performed on the sending device.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **l2tp congestion-control**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	l2tp congestion-control Example: Router(config)# l2tp congestion-control	Enables L2TP congestion avoidance.

What to Do Next

You may perform the optional task in the “[Verifying L2TP Congestion Avoidance](#)” section.

Verifying L2TP Congestion Avoidance

Perform this task to verify that L2TP congestion avoidance is enabled, to determine the current congestion window size and slow start threshold, and to detect congestion control events.

SUMMARY STEPS

- enable**
- show vpdn tunnel l2tp all**
- debug vpdn l2x-events**

DETAILED STEPS

Step 1 **enable**

Enter this command to enable privileged EXEC mode. Enter your password if prompted:

```
Router> enable
```

Step 2 **show vpdn tunnel l2tp all**

Displays information about all active L2TP VPDN tunnels.

The following example shows L2TP tunnel activity, including the information that L2TP congestion control is enabled. Note that the slow start threshold is set to the same size as the remote receive window size. The bold text highlights the relevant output.

```
Router# show vpdn tunnel l2tp all
```

```
L2TP Tunnel Information Total tunnels 1 sessions 1
```

```
Tunnel id 30597 is up, remote id is 45078, 1 active sessions
```

```

Tunnel state is established, time since change 00:08:27
Tunnel transport is UDP (17)
Remote tunnel name is LAC1
  Internet Address 172.18.184.230, port 1701
Local tunnel name is LNS1
  Internet Address 172.18.184.231, port 1701
Tunnel domain unknown
VPDN group for tunnel is 1
L2TP class for tunnel is
4 packets sent, 3 received
194 bytes sent, 42 received
Last clearing of "show vpdn" counters never
Control Ns 2, Nr 4
Local RWS 500, Remote RWS 500
Control channel Congestion Control is enabled
  Congestion Window size, Cwnd 3
  Slow Start threshold, Ssthresh 500
  Mode of operation is Slow Start
Tunnel PMTU checking disabled
Retransmission time 1, max 2 seconds
Unsent queuesize 0, max 0
Resend queuesize 0, max 1
Total resends 0, ZLB ACKs sent 2
Current nosession queue check 0 of 5
Retransmit time distribution: 0 0 0 0 0 0 0 0
Sessions disconnected due to lack of resources 0
Control message authentication is disabled

```

Step 3 debug vpdn l2x-events

Displays troubleshooting information for protocol-specific VPDN tunneling events.

The following partial output from the **debug vpdn l2x-events** command shows that congestion occurred. The congestion window size and the slow start threshold have been reset due to a packet retransmission event. The bold text highlights the relevant output.

```

Router# debug vpdn l2x-events

!
*Jul 15 19:02:57.963: Tnl 47100 L2TP: Congestion Control event received is retransmission
*Jul 15 19:02:57.963: Tnl 47100 L2TP: Congestion Window size, Cwnd 1
*Jul 15 19:02:57.963: Tnl 47100 L2TP: Slow Start threshold, Ssthresh 2
*Jul 15 19:02:57.963: Tnl 47100 L2TP: Remote Window size, 500
*Jul 15 19:02:57.963: Tnl 47100 L2TP: Control channel retransmit delay set to 4 seconds
*Jul 15 19:03:01.607: Tnl 47100 L2TP: Update ns/nr, peer ns/nr 2/5, our ns/nr 5/2
!

```

The following partial output from the **debug vpdn l2x-events** command shows that traffic has been restarted with L2TP congestion avoidance operating in slow start mode. The bold text highlights the relevant output.

```

Router# debug vpdn l2x-events

!
*Jul 15 14:45:16.123: Tnl 30597 L2TP: Control channel retransmit delay set to 2 seconds
*Jul 15 14:45:16.123: Tnl 30597 L2TP: Tunnel state change from idle to wait-ctl-reply
*Jul 15 14:45:16.131: Tnl 30597 L2TP: Congestion Control event received is positive acknowledgement
*Jul 15 14:45:16.131: Tnl 30597 L2TP: Congestion Window size, Cwnd 2
*Jul 15 14:45:16.131: Tnl 30597 L2TP: Slow Start threshold, Ssthresh 500
*Jul 15 14:45:16.131: Tnl 30597 L2TP: Remote Window size, 500
*Jul 15 14:45:16.131: Tnl 30597 L2TP: Congestion Ctrl Mode is Slow Start
!

```

Configuring VPDN Failure Event Logging

Logging of a failure event to the history table is triggered by event logging by the syslog facility. The syslog facility creates a history failure table, which keeps records of failure events. The table defaults to a maximum of 20 entries, but the size of the table can be configured to retain up to 50 entries.

Failure entries are kept chronologically in the history table. Each entry records the relevant information of a failure event. Only the most recent failure event per user, unique to its name and tunnel client ID (CLID), is kept. When the total number of entries in the table reaches the configured maximum table size, the oldest record is deleted and a new entry is added.

The logging of VPDN failure events to the VPDN history failure table is enabled by default. You need enable VPDN failure event logging only if it has been previously disabled. Perform this task to enable VPDN failure event logging, to configure the maximum number of entries the history failure table can hold, and to display and clear the contents of the VPDN history failure table.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn history failure**
4. **vpdn history failure table-size** *entries*
5. **exit**
6. **show vpdn history failure**
7. **clear vpdn history failure**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><code>enable</code></p> <p>Example: Router> enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<p><code>configure terminal</code></p> <p>Example: Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p><code>vpdn history failure</code></p> <p>Example: Router(config)# vpdn history failure</p>	<p>(Optional) Enables logging of VPDN failure events to the history failure table.</p> <p>Note VPDN history failure logging is enabled by default. You need issue the vpdn history failure command only if you have previously disabled VPDN history failure logging using the no vpdn history failure command.</p>
Step 4	<p><code>vpdn history failure table-size entries</code></p> <p>Example: Router(config)# vpdn history failure table-size 50</p>	<p>(Optional) Sets the history failure table size.</p> <p>Note The VPDN history failure table size may be configured only when VPDN failure event logging is enabled using the vpdn history failure command.</p>
Step 5	<p><code>exit</code></p> <p>Example: Router# exit</p>	<p>Exits to privileged EXEC mode.</p>
Step 6	<p><code>show vpdn history failure</code></p> <p>Example: Router# show vpdn history failure</p>	<p>(Optional) Displays the contents of the history failure table.</p>
Step 7	<p><code>clear vpdn history failure</code></p> <p>Example: Router# clear vpdn history failure</p>	<p>(Optional) Clears the contents of the history failure table.</p>

Enabling Generic VPDN Event Logging

Generic VPDN events are a mixture of error, warning, notification, and information reports logged by the syslog facility. When VPDN event logging is enabled locally or at a remote tunnel endpoint, VPDN event messages are printed to the console as the events occur. VPDN event messages can also be reported to a remote authentication, authorization, and accounting (AAA) server in a AAA vendor-specific attribute (VSA), allowing the correlation of VPDN call success rates with accounting records.

Perform this task to enable generic VPDN event logging.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn logging [accounting | local | remote | tunnel-drop | user]**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	vpdn logging [accounting local remote tunnel-drop user] Example: Router(config)# vpdn logging remote	(Optional) Enables the logging of generic VPDN events . <ul style="list-style-type: none"> • You may configure as many types of generic VPDN event logging as you want by issuing multiple instances of the vpdn logging command. <p>Note The reporting of VPDN event log messages to a AAA server can be enabled independently of all other generic VPDN event logging configurations.</p>

Configuration Examples for VPDN Tunnel Management

This section contains the following configuration examples:

- [Manually Terminating VPDN Tunnels: Examples, page 27](#)
- [Enabling Soft Shutdown of VPDN Tunnels: Example, page 27](#)
- [Configuring VPDN Session Limits: Examples, page 27](#)
- [Verifying Session Limits for a VPDN Group: Example, page 28](#)
- [Configuring L2F Control Packet Timers and Retry Counters for VPDN Tunnels: Example, page 28](#)
- [Configuring L2TP Control Packet Timers and Retry Counters for VPDN Tunnels: Example, page 28](#)
- [Configuring L2TP Congestion Avoidance: Example, page 29](#)
- [Configuring VPDN Failure Event Logging: Example, page 29](#)
- [Configuring Generic VPDN Event Logging: Examples, page 30](#)

Manually Terminating VPDN Tunnels: Examples

The following example manually terminates all L2TP tunnels that terminate on the router:

```
Router# clear vpdn tunnel l2tp all
```

The following example manually terminates the L2F tunnel with the tunnel ID 32:

```
Router# clear vpdn tunnel l2f id 32
```

Enabling Soft Shutdown of VPDN Tunnels: Example

The following example enables soft shutdown of all VPDN tunnels that terminate on the device that the command is issue on:

```
Router# configure terminal
Router(config)# vpdn softshut
Router(config)#
```

```
!The following syslog message will appear on the device whenever an attempt is made to
!establish a new VPDN session after soft shutdown is enabled.
!
00:11:17:%VPDN-6-SOFTSHUT:L2F HGW tunnelserver1 has turned on softshut and rejected user
user2@cisco.com
```

Configuring VPDN Session Limits: Examples

The following example configures a VPDN group named customer7 with a group-level session limit of 25. No more than 25 sessions may be associated with this VPDN group.

```
Router(config)# vpdn-group customer7
Router(config-vpdn)# session-limit 25
```

A VPDN template named customer4 is then created, and a session limit of 8 is configured at the VPDN template-level. Two VPDN groups are associated with the VPDN template, each with a VPDN group-level session limit of 5.

```
Router(config)# vpdn-template customer4
Router(config-vpdn-templ)# group session-limit 8
!
Router(config)# vpdn-group customer4_l2tp
Router(config-vpdn)# source vpdn-template customer4
Router(config-vpdn)# session-limit 5
!
Router(config)# vpdn-group customer4_l2f
Router(config-vpdn)# source vpdn-template customer4
Router(config-vpdn)# session-limit 5
```

With this configuration, if the VPDN group named customer4_l2tp has 5 active sessions, the VPDN group named customer4_l2f may establish only 3 sessions. The VPDN group named customer7 may still have up to 25 active sessions.

If a global limit of 16 VPDN sessions is also configured, the global limit takes precedence over the configured VPDN group and VPDN template session limits.

```
Router# configure terminal
Router(config)# vpdn session-limit 16
```

The three VPDN groups will be able to establish a total of 16 sessions between them. For example, if the VPDN group named customer4_l2tp has the maximum allowable number of active sessions (5 sessions), and the VPDN group named customer4_l2f has 2 active sessions, the VPDN group named customer7 may establish only up to 9 sessions.

Verifying Session Limits for a VPDN Group: Example

The following example creates the VPDN group named l2tp and restricts it to three sessions. The configured session limit is displayed when the **show vpdn group** command is issued.

```
Router# configure terminal
Router(config)# vpdn-group l2tp
Router(config-vpdn)# accept dialin
Router(config-vpdn-acc-in)# protocol l2tp
Router(config-vpdn-acc-in)# virtual-template 5
Router(config-vpdn-acc-in)# exit
Router(config-vpdn)# terminate-from hostname host1
Router(config-vpdn)# session-limit 3
Router(config-vpdn)# end
Router# show vpdn group l2tp
```

```
Tunnel (L2TP)
-----
dnis:cg1
dnis:cg2
dnis:jan
cisco.com
```

Endpoint	Session Limit	Priority	Active Sessions	Status	Reserved Sessions
172.21.9.67	3	1	0	OK	-
Total	*		0		0

Configuring L2F Control Packet Timers and Retry Counters for VPDN Tunnels: Example

The following example configures all of the available L2F control packet timers and retry counters for the VPDN group named l2f:

```
Router# configure terminal
Router(config)# vpdn-group l2f
Router(config-vpdn)# l2f tunnel timeout setup 25
Router(config-vpdn)# l2f tunnel retransmit initial retries 5
Router(config-vpdn)# l2f tunnel busy timeout 90
Router(config-vpdn)# l2f tunnel retransmit retries 10
```

Configuring L2TP Control Packet Timers and Retry Counters for VPDN Tunnels: Example

The following example configures custom values for all of the available L2TP control packet parameters for the VPDN group named l2tp:

```
Router# configure terminal
Router(config)# vpdn-group l2tp
```

```

Router(config-vpdn)# l2tp tunnel hello 90
Router(config-vpdn)# l2tp tunnel receive window 500
Router(config-vpdn)# l2tp tunnel retransmit retries 8
Router(config-vpdn)# l2tp tunnel retransmit timeout min 2
Router(config-vpdn)# l2tp tunnel timeout no-session 500
Router(config-vpdn)# l2tp tunnel timeout setup 25
Router(config-vpdn)# l2tp tunnel zlbg delay 4
Router(config-vpdn)# l2tp tunnel retransmit initial timeout min 2
Router(config-vpdn)# l2tp tunnel retransmit initial retries 5
Router(config-vpdn)# l2tp tunnel busy timeout 90

```

Configuring L2TP Congestion Avoidance: Example

The following example configures a basic dial-in L2TP VPDN tunnel, sets the receive window size to 500 on the tunnel server (the receiving device), and enables L2TP congestion avoidance on the NAS (the sending device):

Tunnel Server Configuration

```

Router(config)# vpdn enable
!
Router(config)# vpdn-group 1
Router(config-vpdn)# accept-dialin
Router(config-vpdn-acc-in)# protocol l2tp
Router(config-vpdn-acc-in)# virtual-template 1
!
Router(config-vpdn)# terminate from hostname NAS1
Router(config-vpdn)# l2tp tunnel receive-window 500

```

NAS Configuration

```

Router(config)# vpdn enable
!
Router(config)# vpdn-group 1
Router(config-vpdn)# request-dialin
Router(config-vpdn-req-in)# protocol l2tp
Router(config-vpdn-req-in)# domain cisco.com
!
Router(config-vpdn)# initiate-to ip 172.22.66.25
Router(config-vpdn)# local name NAS1
!
Router(config)# l2tp congestion-control

```

Configuring VPDN Failure Event Logging: Example

The following example first disables and then reenables VPDN failure event logging, and sets the maximum number of entries in the VPDN history failure table to 50. The contents of the history failure table are displayed and then cleared.

```

Router# configure terminal
Router(config)# no vpdn history failure
Router(config)# vpdn history failure
Router(config)# vpdn history failure table-size 50
Router(config)# end
Router# show vpdn history failure
!
Table size: 50
Number of entries in table: 1
User: user@cisco.com, MID = 1

```

```
NAS: isp, IP address = 172.21.9.25, CLID = 1
Gateway: hp-gw, IP address = 172.21.9.15, CLID = 1
Log time: 13:08:02, Error repeat count: 1
Failure type: The remote server closed this session
Failure reason: Administrative intervention
!
Router# clear vpdn history failure
```

Configuring Generic VPDN Event Logging: Examples

The following example enables VPDN logging locally:

```
Router# configure terminal
Router(config)# vpdn logging local
```

The following example disables VPDN event logging locally, enables VPDN event logging at the remote tunnel endpoint, and enables the logging of both VPDN user and VPDN tunnel-drop events to the remote router:

```
Router# configure terminal
Router(config)# no vpdn logging local
Router(config)# vpdn logging remote
Router(config)# vpdn logging user
Router(config)# vpdn logging tunnel-drop
```

The following example disables the logging of VPDN events at the remote tunnel endpoint, and enables the logging of VPDN event log messages to the AAA server:

```
Router# configure terminal
Router(config)# no vpdn logging local
Router(config)# no vpdn logging remote
Router(config)# vpdn logging accounting
```

Additional References

The following sections provide references related to VPDN tunnel management.

Related Documents

Related Topic	Document Title
VPDN technology overview	“VPDN Technology Overview”
VPDN commands: complete command syntax, command mode, defaults, usage guidelines, and examples	Cisco IOS VPDN Command Reference , Release 12.4T
Technical support documentation for VPDNs	Virtual Private Dial-up Network (VPDN)
Dial Technologies commands: complete command syntax, command mode, defaults, usage guidelines, and examples	Cisco IOS Dial Technologies Command Reference , Release 12.4T

Standards

Standards	Title
TCP/IP; slow start and congestion avoidance algorithms	<i>TCP/IP Illustrated, Volume 1</i> , by W Richard Stevens

MIBs

MIBs	MIBs Link
<ul style="list-style-type: none"> CISCO-VPDN-MGMT-MIB CISCO-VPDN-MGMT-EXT-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

RFCs

RFCs	Title
RFC 2341	Cisco Layer Two Forwarding (Protocol) “L2F”
RFC 2637	Point-to-Point Tunneling Protocol (PPTP)
RFC 2661	<i>Layer Two Tunneling Protocol “L2TP”</i>

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of 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/techsupport

Feature Information for VPDN Tunnel Management

Table 1 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Releases 12.2(1) or a later release appear in the table.

Not all commands may be available in your Cisco IOS software release. For details on when support for specific commands was introduced, see the command reference documents.

If you are looking for information on a feature in this technology that is not documented here, see the “[VPDN Features Roadmap](#).”

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. 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.

Table 1 Feature Information for VPDN Tunnel Management

Feature Name	Software Releases	Feature Configuration Information
VPDN Extended Failover	12.2(34)SB 12.2(31)ZV 12.2(33)SRE	Enables a failover with an LNS, if the LNS receives a valid L2TP CDN or stopCNN message before the LNS establishes a session. The following section provides information about this feature: <ul style="list-style-type: none"> • VPDN Extended Failover, page 3
L2TP Congestion Avoidance	12.2(28)SB	This feature provides packet flow control and congestion avoidance by throttling Layer 2 Transport Protocol (L2TP) control messages as described in RFC 2661. The following sections provide information about this feature: <ul style="list-style-type: none"> • L2TP Congestion Avoidance, page 3 • Configuring L2TP Congestion Avoidance, page 19 The following commands were introduced or modified by this feature: debug vpdn, l2tp congestion-control .
Session Limit per VRF	12.2(13)T	This feature allows you to apply session limits on all VPDN groups associated with a common VPDN template. You can limit the number of VPDN sessions that terminate in a single VPN Routing and Forwarding (VRF) instance. The following sections provide information about this feature: <ul style="list-style-type: none"> • VPDN Session Limits, page 2 • Limiting the Number of Allowed Simultaneous VPDN Sessions, page 9 The following commands were introduced or modified by this feature: group session-limit, source vpdn-template, vpdn-template .

Table 1 Feature Information for VPDN Tunnel Management (continued)

Feature Name	Software Releases	Feature Configuration Information
Timer and Retry Enhancements for L2TP and L2F	12.2(4)T 12.2(28)SB	<p>This feature allows the user to configure certain adjustable timers and counters for L2TP and L2F.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Control Packet Parameters for VPDN Tunnels, page 3 • Configuring L2F Control Packet Parameters for VPDN Tunnels, page 17 • Configuring L2TP Control Packet Parameters for VPDN Tunnels, page 13 <p>The following commands were introduced by this feature: l2f tunnel busy timeout, l2f tunnel retransmit initial retries, l2f tunnel retransmit retries, l2f tunnel timeout setup, l2tp tunnel busy timeout, l2tp tunnel retransmit initial retries, l2tp tunnel retransmit initial timeout.</p>
VPDN Group Session Limiting	12.2(4)T 12.2(28)SB	<p>This feature allows the user to configure a limit on the number of L2F or L2TP VPDN sessions allowed for each VPDN group.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • VPDN Session Limits, page 2 • Limiting the Number of Allowed Simultaneous VPDN Sessions, page 9 • Verifying VPDN Session Limits, page 12 <p>The following command was introduced by this feature: session-limit (VPDN).</p>

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CDDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0910R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2008 Cisco Systems, Inc. All rights reserved.

