

# VPN Tunnel Management

---

This feature module describes the Virtual Private Network (VPN) feature. It includes information on the benefits of the new feature, supported platforms, related documents, and so forth.

This document includes the following sections:

- Feature Overview, page 1
- Supported Platforms, page 2
- Supported Standards, MIBs, and RFCs, page 3
- Configuration Tasks, page 3
- Monitoring and Maintaining VPN sessions, page 5
- Configuration Examples, page 6
- Command Reference, page 7

## Feature Overview

The VPN Tunnel Management feature provides network administrators with two new functions for managing VPN tunnels:

- The ability to set a limit for the maximum number of allowed simultaneous VPN sessions
- The ability to prevent new sessions from being established on a VPN tunnel without disturbing the service of existing sessions (this function is called VPN tunnel soft shutdown)

These functions can be used on either end of a VPN tunnel—the Network Access Server (NAS) or on the tunnel server.

When this feature is enabled, Multichassis Multilink PPP (MMP) Layer 2 Forwarding (L2F) tunnels can still be created and established.

### NAS VPN Tunnel Soft Shutdown

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

### Tunnel Server VPN Tunnel Soft Shutdown

When this feature is enabled on a tunnel server, the reason for the session refusal will be returned to the NAS. This information is recorded in the VPN history failure table.

## Benefits

The VPN Tunnel Management feature gives network administrators greater flexibility in managing VPN traffic. It enables network administrators to prevent a VPN tunnel from becoming congested without affecting previously established sessions.

## Related Documents

For more information about Cisco VPN, see the following documents:

- The *Layer 2 Tunnel Protocol* feature module, which is located under *New Features in Release 12.0(1)T* from CCO.
- The following feature modules located under *New Features in Release 12.0(5)T* from CCO:
  - *L2TP Dialout*
  - *L2TP Tunnel Preservation of IP TOS*
  - *Resource Pool Management*
  - *VPDN Group Reorganization*
  - *VPDN Per-User Configuration*
- The “Virtual Private Dialup Network” chapter in the *Dial Solutions Configuration Guide*.
- The *Access VPN Solutions Using Tunneling Technology* solutions guide, which is located under the *Internetworking Solutions Guides* index on CCO’s documentation home page.

## Supported Platforms

- Cisco 1600 series
- Cisco 1720 VPN Access Router
- Cisco 2500 series
- Cisco 2600 series
- Cisco 3600 series
- Cisco 4000-M series (Cisco 4000-M, 4500-M, 4700-M)
- Cisco 7000 series
- Cisco 7100 series
- Cisco 7200 series
- Cisco 7500 series
- Cisco AS5200
- Cisco AS5300
- Cisco AS5800

## Supported Standards, MIBs, and RFCs

### Standards

None

### MIBs

- CISCO-VPDN-MGMT-MIB.my
- CISCO-VPDN-MGMT-MIB-VISMI.my

For descriptions of supported MIBs and how to use MIBs, see the Cisco MIB web site on CCO at <http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>.

### RFCs

- L2TP RFC

## Configuration Tasks

See the following sections for configuration tasks for the VPN Tunnel Management feature. Each task in the list indicates if the task is optional or required.

- Limiting the Number of Allowed Simultaneous VPN Sessions (Required)
- Enabling Soft Shutdown of VPN Tunnels (Required)

## Limiting the Number of Allowed Simultaneous VPN Sessions

Command	Purpose
<code>great_went(config)# vpdn session-limit sessions</code>	Limits the number of simultaneous VPN <sup>1</sup> sessions on the router to the number specified with the <i>sessions</i> argument.

<sup>1</sup> The Cisco IOS command syntax uses the more specific term virtual private dialup network (VPDN) instead of VPN.

## Enabling Soft Shutdown of VPN Tunnels

Command	Purpose
<code>great_went(config)# vpdn softshut</code>	Prevents new sessions from being established on a VPN tunnel without disturbing existing sessions.

## Verifying Simultaneous VPN Session Limits

- Step 1** Enter the **terminal monitor** privileged EXEC command.
- Step 2** Enter the **vpdn session-limit 1** global configuration command on either the NAS or tunnel server.
- Step 3** Establish a VPN session by dialing in to the NAS using an allowed username and password.

**Step 4** Attempt to establish another VPN session.

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 great_went has exceeded configured local
session-limit and rejected user wilson@soam.com
```

**Step 5** Enter the **show vpdn history failure** command on the router. If you see output similar to the following, the session limit was successful:

```
User:wilson@soam.com
NAS:cliford_ball, IP address = 172.25.52.8, CLID = 2
Gateway:great_went, 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.
Failure reason:
```

## Verifying Soft Shutdown of VPN Tunnels

**Step 1** Enter the **terminal monitor** privileged EXEC command.

**Step 2** Establish a VPN session by dialing in to the NAS using an allowed username and password.

**Step 3** Enter the **vpdn softshut** global configuration command on either the NAS or tunnel server.

**Step 4** Verify that the original session is still active by entering the **show vpdn** command:

```
ENT_HGW# show vpdn
% No active L2TP tunnels

L2F Tunnel and Session

NAS CLID HGW CLID NAS Name          HGW Name          State
36      1      cliford_ball    great_went        open
                172.25.52.8     172.25.52.7

CLID  MID  Username                               Intf  State
36    1    mockingbird@gamehendge.com           Vi1   open
```

**Step 5** Attempt to establish another VPN session.

A Syslog message similar to the following should appear on the console of the soft shutdown router:

```
00:11:17:%VPDN-6-SOFTSHUT:L2F HGW great_went has turned on softshut and rejected
user wilson@soam.com
```

**Step 6** Enter the **show vpdn history failure** command on the soft shutdown router. If you see output similar to the following, the soft shutdown was successful:

```
User:wilson@soam.com
NAS:cliford_ball, IP address = 172.25.52.8, CLID = 2
Gateway:great_went, IP address = 172.25.52.7, CLID = 13
Log time:00:04:21, Error repeat count:1
Failure type:VPDN softshut has been activated.
Failure reason:
```

The following EXEC commands provide useful information for verifying VPN sessions:

<b>show interface virtual access</b> <i>number</i>	Displays information about the virtual access interface, Link Control Protocol (LCP), protocol states, and interface statistics. The status of the virtual access interface should be: "Virtual-Access3 is up, line protocol is up"
<b>show vpdn session</b> [all [interface   tunnel   username]   packets   sequence   state   timers   window]	Displays VPN session information including interface, tunnel, username, packets, status, and window statistics.
<b>show vpdn tunnel</b> [all [id   local-name   remote-name]   packets   state   summary   transport]	Displays VPN tunnel information including tunnel protocol, ID, local and remote tunnel names, packets sent and received, tunnel, and transport status.

## Monitoring and Maintaining VPN sessions

The following EXEC commands will help you monitor and maintain VPN sessions:

Command	Purpose
<b>clear vpdn tunnel</b> [l2f [nas-name   hgw-name]   l2tp [remote-name   local-name]]	Shuts down a specific tunnel and all the sessions within the tunnel.
<b>debug dialer events</b>	Displays information about packets received on dialer interfaces.
<b>debug ppp chap</b>	Displays CHAP packet exchanges.
<b>debug ppp negotiation</b>	Displays information about packets sent during PPP startup and detailed PPP negotiation options.
<b>debug vpdn event</b> [protocol   flow-control]	Displays VPN errors and basic events within the protocol (such as L2TP, L2F, PPTP) and errors associated with flow control. Flow control is only possible if you are using L2TP and the remote peer "receive window" is configured for a value greater than zero.
<b>debug vpdn packet</b> [control   data] [detail]	Displays protocol-specific packet header information, such as sequence numbers if present, flags, and length.

The following EXEC commands will provide more detailed information about VPN sessions:

Command	Purpose
<b>debug aaa authentication</b>	Displays information on AAA authentication.
<b>debug aaa authorization</b>	Displays information on AAA authorization.
<b>debug vpdn l2x-errors</b>	Displays L2F and L2TP protocol errors that prevent tunnel establishment or normal operation.
<b>debug vpdn l2x-events</b>	Displays L2F and L2TP events that are part of tunnel establishment or shutdown.

## Configuration Examples

This section provides the following configuration examples:

- NAS Configured for Dial-In with VPN Tunnel Management
- Tunnel Server Configured for Dial-In with VPN Tunnel Management

### NAS Configured for Dial-In with VPN Tunnel Management

The following example shows a NAS configured to accept L2F dial-in. It is configured to allow a maximum of ten simultaneous VPN sessions, and has the **vpdn softshut** command enabled:

```
aaa new-model
aaa authentication ppp default local
aaa authorization network default local
!
username ISP_NAS password 7 tunnelme
username ENT_HGW password 7 tunnelme
!
vpdn enable
!
vpdn session-limit 10
vpdn softshut
vpdn-group 1
  accept dialin
  protocol l2f
  virtual-template 1
  terminate-from hostname ISP_NAS
  local name ENT_HGW
!
interface FastEthernet0/0
ip address 172.25.52.8 255.255.255.192
no ip directed-broadcast
!
interface Virtual-Template1
ip unnumbered FastEthernet0/0
peer default ip address pool default
ppp authentication chap
!
ip local pool default 172.30.2.1 172.30.2.96
```

## Tunnel Server Configured for Dial-In with VPN Tunnel Management

The following example shows a tunnel server configured to request L2F dial-in. It is configured to allow a maximum of ten simultaneous VPN sessions, and has the **vpdn softshut** command enabled:

```
aaa new-model
aaa authentication ppp default local
aaa authorization network default local
!
username ISP_NAS password 7 tunnelme
username ENT_HGW password 7 tunnelme
!
vpdn enable
!
vpdn search-order domain dnis
vpdn session-limit 10
vpdn softshut
vpdn-group 1
  request dialin
  protocol l2f
  domain soam.com
  initiate-to ip 172.25.52.8
  local name ISP_NAS
!
controller T1 0
  framing esf
  clock source line primary
  linecode b8zs
  pri-group timeslots 1-24
!
interface Ethernet0
  ip address 172.25.52.7 255.255.255.192
```

## Command Reference

This section documents new commands. All other commands used with this feature are documented in the Cisco IOS Release 12.0 command reference publications.

- **vpdn session-limit**
- **vpdn softshut**

## vpdn session-limit

To limit the number of simultaneous VPN sessions that can be established on a router, use the **vpdn session-limit** command. To allow an unlimited number of simultaneous VPN sessions, use the **no** form of this command.

**vpdn session-limit** *sessions*

**no vpdn session-limit**

### Syntax Description

*sessions* The maximum number of simultaneous VPN sessions that are allowed on a router.

### Defaults

Disabled

### Command Modes

Global configuration

### Command History

Release	Modification
12.0(7)T	This command was introduced.

### Usage Guidelines

When this command is enabled, use the **show vpdn history failure** command to view records of refused attempts to establish new sessions.

### Examples

The following example first sets a limit of two simultaneous VPN sessions on the router and then shows a Syslog message stating that an attempt to establish a new session was refused:

```
great_went(config)# vpdn session-limit 2
great_went(config)#
00:11:17:%VPDN-6-MAX_SESS_EXCD:L2F HGW great_went exceeded configured local
session-limit and rejected user wilson@soam.com
great_went(config)#
```

### Related Commands

Command	Description
<b>show vpdn history failure</b>	Displays the content of the failure history table.
<b>vpdn softshut</b>	Prevents new sessions from being established on a VPN tunnel without disturbing existing sessions.

## vpdn softshut

To prevent new sessions from being established on a VPN tunnel without disturbing existing sessions, use the **vpdn softshut** global configuration command. To return the VPN tunnel to active service, use the **no** form of this command.

```
vpdn softshut
no vpdn softshut
```

### Syntax Description

This command has no arguments or keywords.

### Defaults

Disabled

### Command Modes

Global configuration

### Command History

Release	Modification
12.0(5)T	This command was introduced.

### Usage Guidelines

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

When this feature is enabled on a tunnel server, the reason for the session refusal will be returned to the NAS. This information is recorded in the VPN history failure table.

When this command is enabled, use the **show vpdn history failure** command to view records of refused attempts to establish new sessions.

### Examples

The following example first enables the **vpdn softshut** command and then shows a Syslog message stating that an attempt to establish a new session was refused:

```
great_went(config)# vpdn softshut
great_went(config)#
00:11:17:%VPDN-6-SOFTSHUT:L2F HGW great_went has turned on softshut and rejected user
wilson@soam.com
great_went(config)#
```

### Related Commands

<b>Command</b>	<b>Description</b>
<b>show vpdn history failure</b>	Displays the content of the failure history table.
<b>vpdn session-limit</b>	Limits the number of simultaneous VPN sessions that can be established on a router.