



## Session Limit per VPDN Template

The Session Limit per VPDN Template feature allows you to apply session limits on all VPDN groups associated with a common virtual private dialup network (VPDN) template. You can limit the number of VPDN sessions that terminate in a single VRF.

### Feature Specifications for the Session Limit per VPDN Template Feature

#### Feature History

Release	Modification
12.2(4)B	This feature was introduced on the Cisco 7200 series routers and the Cisco 7401ASR router.
12.2(13)T	This feature was integrated into Cisco IOS Release 12.2(13)T and support was added for the following platforms: Cisco 2600 series, Cisco 3620 series, Cisco 3640 series, Cisco 3660 series, Cisco 5300 series, Cisco 5350 series, Cisco 5400 series, Cisco 5800 series, Cisco 5850 series, Cisco 6400 series, Cisco 7200 series, Cisco 7400 series, Cisco 7500 series

#### Supported Platforms

For platforms supported in Cisco IOS Release 12.2(13)T, consult Cisco Feature Navigator.

### Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that are supported on specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to [cco-locksmith@cisco.com](mailto:cco-locksmith@cisco.com). An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

<http://www.cisco.com/go/fn>

### Availability of Cisco IOS Software Images

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, refer to the online release notes or, if supported, Cisco Feature Navigator.

## Contents

- [Prerequisites for Session Limit per VPDN Template, page 2](#)
- [Restrictions for Session Limit per VPDN Template, page 2](#)
- [Information About Session Limit per VPDN Template, page 2](#)
- [How to Configure Session Limit per VPDN Template, page 3](#)
- [Configuration Examples for Session Limit per VPDN Template, page 8](#)
- [Additional References, page 10](#)
- [Command Reference, page 11](#)
- [Glossary, page 19](#)

## Prerequisites for Session Limit per VPDN Template

To enable the Session Limit per VPDN Template feature, you must have a VPDN enabled on the router and at least one VPDN group configured. The router must make a Level 2 Forwarding (L2F) or Layer 2 Tunneling Protocol (L2TP) connection before VPDN configurations can be established.

## Restrictions for Session Limit per VPDN Template

Nesting of VPDN templates is not supported. A single VPDN group can be associated only with one template at a time.

## Information About Session Limit per VPDN Template

To configure the Session Limit per VPDN Template feature, you should understand the following concepts:

- [Benefits of Session Limit per VPDN Template, page 3](#)
- [How Session Limit per VPDN Template Works, page 3](#)

## Benefits of Session Limit per VPDN Template

The Session Limit per VPDN Template feature controls the resources consumed by a single customer account by limiting the number of concurrent sessions terminating in a single VPN Routing and Forwarding (VRF).

## How Session Limit per VPDN Template Works

Before the implementation of the Session Limit per VPDN Template feature, a single default template carrying the configuration values of a subset of VPDN group commands were associated with all VPDN groups configured on the router. The Session Limit per VPDN Template feature allows you to limit the number of VPDN sessions terminated on a single VRF by allowing for session limits to be applied on all VPDN groups associated with a common virtual private dialup network (VPDN) template.

The Session Limit per VPDN Template feature enables you to create, define, and name multiple VPDN templates. You can then associate a specific template that matches VRF requirements with a VPDN group. A session limit can be configured at the VPDN template level to specify a combined session limit for all VPDN groups associated with the configured VPDN template.

## How to Configure Session Limit per VPDN Template

This section contains the following procedures:

- [Configuring Session Limit per VPDN Template, page 3](#) (required)
- [Monitoring and Maintaining Session Limit per VPDN Template, page 6](#) (optional)

## Configuring Session Limit per VPDN Template

Perform this task to configure the Session Limit per VPDN Template.

### SUMMARY STEPS

1. **vpdn enable**
2. **vpdn-template** *name*
3. **group session-limit** *number*
4. Repeat Steps 2 and 3 to configure additional named VPDN templates.
5. **exit**
6. **vpdn-group** *tag*
7. **accept-dialin**  
or  
**request-dialout**
8. **protocol** *protocol*
9. **exit**
10. **source vpdn-template** *name*

11. Repeat Steps 6 through 10 to configure session limiting on additional VPDN groups.

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>vpdn enable</code>  <b>Example:</b> Router(config)# <code>vpdn enable</code>	Enables virtual private dialup networking on the router and informs the router to look for tunnel definitions in a local database and on a remote authorization server (home gateway), if one is present.
Step 2	<code>vpdn-template name</code>  <b>Example:</b> Router(config)# <code>vpdn-template template-a</code>	Enters VPDN group configuration mode to configure a VPDN template.  <ul style="list-style-type: none"> <li><code>name</code>—The name of the VPDN template to be associated with this VPDN group.</li> </ul>
Step 3	<code>group session-limit number</code>  <b>Example:</b> Router(config- <i>vpdn</i> )# <code>group session-limit 10</code>	Specifies the maximum number of concurrent sessions allowed across all VPDN groups associated with the VPDN template specified in Step 2.  <ul style="list-style-type: none"> <li><code>number</code>—Valid values are from 1 to 32767.</li> </ul>
Step 4	Repeat Steps 2 and 3 to configure additional named VPDN templates.	—
Step 5	<code>exit</code>  <b>Example:</b> Router(config- <i>vpdn</i> )# <code>exit</code>	Exits VPDN group configuration mode.
Step 6	<code>vpdn-group tag</code>  <b>Example:</b> Router(config)# <code>vpdn-group small-group</code>	Associates a VPDN group to a customer or VPDN profile.  <ul style="list-style-type: none"> <li><code>tag</code>—Name of the VPDN group.</li> </ul>
Step 7	<code>accept-dialin</code>  or <code>request-dialout</code>  <b>Example:</b> Router(config- <i>vpdn</i> )# <code>accept-dialin</code>  or Router(config- <i>vpdn</i> )# <code>request-dialout</code>	Enables the router to accept dial-in requests and enters VPDN accept-dialin group configuration mode.  or Enables the router to send L2TP dial-out requests and enters VPDN request-dialout group configuration mode.
Step 8	<code>protocol protocol</code>  <b>Example:</b> Router(config- <i>vpdn-acc-in</i> )# <code>protocol any</code>  or Router(config- <i>vpd-req-out</i> )# <code>protocol any</code>	Specifies which tunneling protocol is to be used.

	Command or Action	Purpose
Step 9	<b>exit</b>  <b>Example:</b> Router(config-vpd-acc-in)# <b>exit</b> or Router(config-vpd-req-out)# <b>exit</b>	Exits VPDN accept-dialin group configuration mode.  or  Exits VPDN request-dialout group configuration mode.
Step 10	<b>source vpdn-template name</b>  <b>Example:</b> Router(config)# <b>source vpdn-template primary</b>	Configures the VPDN group to use the VPDN template settings for all unspecified parameters. <ul style="list-style-type: none"> <li><i>name</i>—The name of the VPDN template to be associated with a VPDN-group.</li> </ul>
Step 11	Repeat Steps 6 through 10 to configure session limiting on additional VPDN groups.	—

## Output Examples

This section shows you how to verify your configuration of the Session Limit per VPDN Template feature:

- [Sample Output for the show running-config command, page 5](#)

## Sample Output for the show running-config command

Enter the **show running-config** command to verify the configuration of the Session Limit per VRF feature:

```
Router# show running-config

Building configuration...

Current configuration :2655 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname lns
!
logging buffered 64000 debugging
no logging console
aaa new-model
!
!
aaa group server radius vpdn-group
 server 172.16.0.0 auth-port 1645 acct-port 1646
!
aaa authentication ppp default local
aaa authorization network default local
aaa accounting send stop-record authentication failure
aaa accounting network default start-stop group radius
aaa session-id common
!
username client@cisco.com password 0 cisco
username lac password 0 cisco
```

```

username lns password 0 cisco
ip subnet-zero
!
!
no ip domain-lookup
!
ip cef
!
sgbp group cp6512
vpdn enable
vpdn multihop
vpdn tunnel authorization password 7 040B521005255F58031D161D141D03003925223E3C31311D0818
vpdn tunnel authorization virtual-template 200
vpdn tunnel authorization network jkads
!
vpdn-template primary <! This output confirms the configuration of a VPDN template group
"primary">
  group session-limit 3
!
vpdn-group dialout
  accept-dialout
  protocol l2tp
  dialer 1
  terminate-from hostname lac
!
vpdn-group special
! Default L2TP VPDN group
! Default PPTP VPDN group
  accept-dialin
  protocol any
  source vpdn-template primary
!

```

Enter the **show vpdn session** command to display the status of all active tunnels:

```

Router# show vpdn session

%No active L2TP tunnels
L2F Session Information Total tunnels 1 sessions 2

  CLID   MID   Username                Intf      State
  ----   ---   -
  1       4     username@cisco.com      Vi2       open
  1       3     username@cisco.com      Vi1       open

%No active PPTP tunnels
%No active PPPoE tunnels

```

## Monitoring and Maintaining Session Limit per VPDN Template

You may, optionally, verify or troubleshoot performance by performing any of the following steps, in any order.

### SUMMARY STEPS

1. **show vpdn group *name***
2. **show vpdn**
3. **show vpdn history failure**
4. **show vpdn session [all [interface | tunnel | username] | packets | sequence | state | timers | window]**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<pre>show vpdn group name</pre> <p><b>Example:</b> Router# <code>show vpdn group group-b</code></p>	<p>Displays the session limit set, and the number of active sessions and tunnels on the specified VPDN group.</p> <ul style="list-style-type: none"> <li><i>name</i>—VPDN group name that summarizes the configuration of the specified group.</li> </ul>
Step 2	<pre>show vpdn</pre> <p><b>Example:</b> Router# <code>show vpdn</code></p>	<p>Displays a summary of all active VPDN tunnels.</p>
Step 3	<pre>show vpdn history failure</pre> <p><b>Example:</b> Router# <code>show vpdn history failure</code></p>	<p>Displays information about VPDN user failures.</p>
Step 4	<pre>show vpdn session [all [interface   tunnel   username]   packets   sequence   state   timers   window]</pre> <p><b>Example:</b> Router# <code>show vpdn session [all [interface   tunnel   username]   packets   sequence   state   timers   window]</code></p>	<p>Displays VPDN session information including interface, tunnel, username, packets, status, and window statistics:</p> <ul style="list-style-type: none"> <li><b>all</b>—All session information for active sessions <ul style="list-style-type: none"> <li><b>interface</b>—Interface associated to a specific session</li> <li><b>tunnel</b>—Tunnel attribute filter</li> <li><b>username</b>—Username filter</li> </ul> </li> <li><b>packets</b>—Packet or byte count</li> <li><b>sequence</b>—Sequence numbers</li> <li><b>state</b>—State of each session</li> <li><b>timers</b>—Timer information</li> </ul> <p><b>window</b>—Window information</p>
Step 5	<pre>source vpdn-template name</pre> <p><b>Example:</b> Router(config)# <code>vpdn-template group-b</code></p>	<p>Configures the VPDN group to use the VPDN template settings for all unspecified parameters.</p> <ul style="list-style-type: none"> <li><i>name</i>—The name of the VPDN template to be associated with a VPDN-group.</li> </ul>

## Troubleshooting Tips

- If you attempt to associate a VPDN group with a named VPDN template that has not been configured, the VPDN group uses the system defaults.
- You can associate a VPDN group with only one named VPDN template at a time. If you associate a VPDN group with a named VPDN template, and then with a second VPDN template, the VPDN group is unbound from the first VPDN template and associated with the second.
- If you configure the **session-limit** command, it takes precedence over the **group session-limit** command.
- If you configure the **group session-limit** command to allow fewer sessions than are currently active on the router, existing sessions are not brought down and new sessions cannot start.

- If you configure the **vpdn session-limit** command in global configuration mode, these parameters are applied for any settings not configured in the individual VPDN group or VPDN template.
- If you remove a named VPDN template that has VPDN groups associated with it, those VPDN groups are unbound from that VPDN template and are associated with the default VPDN template.

## Configuration Examples for Session Limit per VPDN Template

This section provides the following configuration examples:

- [Configuring Session Limit per VPDN Template Examples, page 8](#)

### Configuring Session Limit per VPDN Template Examples

In the following example, three VPDN groups are created called small-group, medium-group, and large-group. The small-group and medium-group VPDN groups are attached to the default VPDN template. Together, VPDN small-group and medium-group can have no more than ten concurrent sessions. If the small-group has three sessions, the medium-group can have only seven.

VPDN group small-group is configured to have no more than five sessions via the **session-limit 5** command, which leaves at least five sessions available for the medium-group. Because it is part of the VPDN default template group, which has a session limit of ten, the medium-group is still limited to ten sessions (when the small-group has no active sessions), even though the **session-limit 20** command has been configured.

The third VPDN group in this example, large-group, has no session limit configured. It has been detached from the default VPDN template by the **no source vpdn-template** command.

```
vpdn-template
group session-limit 10
exit

vpdn-group medium-group
accept-dialin
protocol any
exit
session-limit 20
exit

vpdn-group small-group
accept-dialin
protocol any
exit
session-limit 5
vpdn-group large-group
accept-dialin
protocol any
exit
no source vpdn-template
```

In the following example the VPDN group called group-c is attached to the default VPDN template. It can have no more than ten concurrent sessions because the **group session-limit 10** command has been configured for the default VPDN template. VPDN group group-c also inherits a local name of local-name from the default VPDN template.

The VPDN groups called group-a and group-b are attached to the VPDN template called template-a. Together, group-a and group-b are limited to 50 concurrent sessions. In addition, group-a and group-b are individually limited to 30 sessions.

Both group-a and group-b VPDN groups use the host name as their local name (host1). Because both group-a and group-b are associated with the VPDN template, template-a, they do not use any configuration from the default VPDN template.

```
hostname host1
vpdn-template
  group session-limit 10
  local name local-name
  exit

vpdn-template template-a
  group session-limit 50
  exit

vpdn-group group-a
  accept-dialin
  protocol any
  exit
  source vpdn-template template-a
  session-limit 30
  exit

vpdn-group group-b
  accept-dialin
  protocol any
  exit
  source vpdn-template template-a
  session-limit 30
  exit

vpdn-group group-c
  accept-dialin
  protocol any
```

In the following example, two VPDN groups are configured, called group-a and group-b. In this example, group-a can have no more than 5 concurrent sessions, even though it has a VPDN group session limit of 20. The configuration of the global VPDN session limit at five sessions takes effect before the larger limit specific to group-a can take effect. Group-b can have no more than two concurrent sessions, even though the global VPDN session-limit is configured for five sessions. The configuration of the VPDN group session limit at two sessions takes effect before the global VPDN session limit can take effect.

```
vpdn session-limit 5

vpdn-template
  group session-limit 10

vpdn-group group-a
  accept-dialin
  protocol any
  exit
  session-limit 20
  exit

vpdn-group group-b
  accept-dialin
  protocol any
  exit
  session-limit 2
```

## Additional References

For additional information related to the Session Limit per VPDN Template feature, refer to the following references:

- [Related Documents, page 10](#)
- [Standards, page 10](#)
- [MIBs, page 10](#)
- [RFCs, page 11](#)

## Related Documents

Related Topic	Document Title
Configuring your Cisco router or access server to support voice, video, and fax applications	<ul style="list-style-type: none"> <li>• <i>Cisco IOS Voice, Video, and Fax Command Reference</i>, Release 12.2</li> <li>• <i>Cisco IOS Voice, Video, and Fax Configuration Guide</i>, Release 12.2</li> </ul>
VPDN group default template	<i>Configuring Virtual Private Dialup Networks</i>
VPDN group session limiting	<i>VPDN Group Session Limiting</i>

## Standards

Standards <sup>1</sup>	Title
None	—

1. Not all supported standards are listed.

## MIBs

MIBs <sup>1</sup>	MIBs Link
None	<p>To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:</p> <p><a href="http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a></p>

1. Not all supported MIBs are listed.

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to [cco-locksmith@cisco.com](mailto:cco-locksmith@cisco.com). An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

## RFCs

RFCs <sup>1</sup>	Title
None	—

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, tools, and lots more. Registered Cisco.com users can log in from this page to access even more content.	<a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a>

## Command Reference

This section documents new and modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.2 command reference publications.

- [group session-limit](#)
- [source vpdn-template](#)
- [vpdn-template](#)

# group session-limit

To specify the maximum concurrent sessions allowed across all virtual private dialup network (VPDN) groups associated with a particular VPDN template, use the **group session-limit** command in VPDN template configuration mode. To disable session limiting for a VPDN template, use the **no** form of this command.

**group session-limit** *number*

**no group session-limit** *number*

<b>Syntax Description</b>	<i>number</i>	Maximum number of concurrent sessions allowed across all VPDN groups associated with a particular VPDN template. Valid values are from 1 to 32767.
---------------------------	---------------	--

**Defaults** No session limit is configured at the VPDN template level.

**Command Modes** VPDN template configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(4)B	This command was introduced.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

**Usage Guidelines** Use this command to specify the maximum concurrent sessions across all VPDN groups associated with a VPDN template. If you configure a group session limit for the default VPDN template, that session limit is the session limit for all VPDN groups not associated with a named VPDN template. The group session limit configured by this command does not terminate active sessions. If you configure a group session limit that is lower than the number of current active sessions, no sessions are terminated and no new sessions can start.

Session limits configured at the VPDN group level by the **session-limit** (VPDN) command take precedence over session limits configured at the VPDN template level when the VPDN group level session limit has a smaller configured value than the VPDN template level.

**Examples** The following example shows how to configure 100 as the maximum number of concurrent sessions across all VPDN groups attached to the VPDN template called template1:

```
vpdn session-limit 100
vpdn-template template1
  group session-limit 50
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>session-limit</b>	Limits the number of VPDN sessions.
<b>session-limit (VPDN)</b>	Limits the number of sessions that are allowed through a specified VPDN group.
<b>show vpdn session</b>	Displays information about active (L2F Protocol tunnel and message identifiers in a VPDN.
<b>source vpdn-template</b>	Configures an individual VPDN group to use VPDN template settings for all unspecified parameters.
<b>vpdn-group</b>	Associates a VPDN group to a customer or VPDN profile.
<b>vpdn session-limit</b>	Limits the number of simultaneous VPN sessions that can be established on a router.
<b>vpdn-template</b>	Enters VPDN group configuration mode to allow the configuration of a VPDN template.

# source vpdn-template

To configure an individual virtual private dialup network (VPDN) group to use VPDN template settings for all unspecified parameters, use the **source vpdn-template** command in VPDN group configuration mode. To configure an individual VPDN group to use system default settings rather than the VPDN template settings for all unspecified parameters, use the **no** form of this command.

**source vpdn-template** [*name*]

**no source vpdn-template** [*name*]

<b>Syntax Description</b>	<i>name</i> (Optional) The name of the VPDN template to be associated with a VPDN group.
---------------------------	--

<b>Defaults</b>	VPDN template settings are applied to individual VPDN groups.
-----------------	---

<b>Command Modes</b>	VPDN group configuration
----------------------	--------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(4)B	This command was introduced.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

<b>Usage Guidelines</b>	<p>Use this command to couple or uncouple individual VPDN groups from the VPDN template. The default hierarchy for the application of VPDN parameters to a VPDN group is as follows:</p> <ul style="list-style-type: none"> <li>VPDN parameters configured for the individual VPDN group are always applied to that VPDN group.</li> <li>VPDN parameters configured in the VPDN template are applied for any settings not specified in the individual VPDN group configuration.</li> <li>System default settings for VPDN parameters are applied for any settings not configured in the individual VPDN group or VPDN template.</li> </ul> <p>Uncoupling an individual VPDN group from the VPDN template using the <b>no source vpdn-template</b> command results in the following hierarchy for the application of VPDN parameters to that individual VPDN group:</p> <ul style="list-style-type: none"> <li>VPDN parameters configured for the individual VPDN group are always applied to that VPDN group.</li> <li>System default settings for VPDN parameters are applied for any settings not configured in the individual VPDN group or VPDN template.</li> </ul> <p>Use the optional <i>name</i> attribute to associate and name a VPDN template with a VPDN group. You can associate a VPDN group with one VPDN template at a time.</p>
-------------------------	--

**Examples**

The following example shows how to configure VPDN group 1 to ignore the VPDN template settings and use the system default settings for all unspecified VPDN parameters:

```
vpdn-group 1
 no source vpdn-template
```

**Related Commands**

Command	Description
<a href="#">group session-limit</a>	Specifies the maximum concurrent sessions allowed across all VPDN groups associated with a particular VPDN template.
<b>session-limit</b>	Limits the number of VPDN sessions.
<b>session-limit (VPDN)</b>	Limits the number of sessions that are allowed through a specified VPDN group.
<b>show vpdn session</b>	Displays information about active L2F Protocol tunnel and message identifiers in a VPDN.
<b>vpdn-group</b>	Associates a VPDN group to a customer or VPDN profile.
<b>vpdn session-limit</b>	Limits the number of simultaneous VPN sessions that can be established on a router.
<a href="#">vpdn-template</a>	Enters VPDN group configuration mode to allow the configuration of a VPDN template.

# vpdn-template

To enter VPDN group configuration mode to configure a virtual private dialup network (VPDN) template, use the **vpdn-template** command in global configuration mode. To inactivate the use of a VPDN template, use the **no** form of this command.

**vpdn-template** *[name]*

**no vpdn-template** *[name]*

## Syntax Description

<i>name</i>	(Optional) The name of the VPDN template to be associated with this VPDN group.
-------------	---

## Defaults

No VPDN template exists. The system default values are applied to individual VPDN groups for any parameters that are not configured in the individual VPDN group.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(4)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

## Usage Guidelines

Use this command to configure global default values for VPDN parameters in a VPDN template. These global default values are applied to all VPDN groups, unless specific values are configured for individual VPDN groups. VPDN parameters that are not specified in the individual VPDN group or in the VPDN template are assigned system default values.

The default hierarchy for the application of VPDN parameters to a VPDN group follows:

- VPDN parameters configured for the individual VPDN group are always applied to that VPDN group.
- VPDN parameters configured in the VPDN template are applied for any settings not specified in the individual VPDN group configuration.
- System default settings for VPDN parameters are applied for any settings not configured in the individual VPDN group or VPDN template.

Not all commands that are available for configuring a VPDN group can be used to configure a VPDN template. [Table 1](#) lists the commands that can be used to configure the VPDN template.

**Table 1** Commands Available for VPDN Template Configuration

Command Name	Description
<b>default</b>	Resets a VPDN command to its default value.
<b>description</b>	Adds a description for a VPDN group.

**Table 1** *Commands Available for VPDN Template Configuration (continued)*

<b>Command Name</b>	<b>Description</b>
<b>exit</b>	Exits VPDN template configuration mode.
<b>ip mtu</b>	Enables the sending of Internet Control Message Protocol (ICMP) redirect messages if the Cisco IOS software is forced to resend a packet through the same interface on which it was received.
<b>ip pmtu</b>	Allows Layer 2 Tunneling Protocol (L2TP) tunnels to participate in path maximum transmission unit (MTU) discovery.
<b>ip precedence</b>	Sets IP Precedence (priority) for packets sent by the dial peer.
<b>ip tos</b>	Specifies the type of service (ToS) level for IP traffic.
<b>l2f ignore-mid-sequence</b>	Ignores message identifier (MID) sequence numbers for sessions in a Layer 2 Forwarding Protocol (L2F) tunnel.
<b>l2f tunnel busy timeout</b>	Configures the amount of time that the router waits before attempting to recontact an L2F destination router that was previously busy.
<b>l2f tunnel retransmit initial retries</b>	Configures the number of times after which a router will stop attempting to send the initial control packet for L2F tunnel establishment to a busy router.
<b>l2f tunnel retransmit retries</b>	Configures the number of times the router will attempt to resend tunnel control packets before tearing down the tunnel.
<b>l2f tunnel timeout setup</b>	Configures the amount of time that the router waits for a confirmation message after sending out the initial control packet to a busy router.
<b>l2tp drop out-of-order</b>	Disables dropping of out-of-sequence packets.
<b>l2tp hidden</b>	Enables L2TP attribute-value (AV) pair hiding, which encrypts the AV pair value.
<b>l2tp ip tos reflect</b>	Configures a VPDN group to preserve the ToS field of L2TP-tunneled IP packets.
<b>l2tp ip udp checksum</b>	Enables IP User Datagram Protocol (UDP) checksums on L2TP payload packets.
<b>l2tp sequencing</b>	Enables L2TP sequencing.
<b>l2tp tunnel authentication</b>	Enables L2TP tunnel authentication.
<b>l2tp tunnel busy timeout</b>	Configures the amount of time that the router waits before attempting to recontact an L2TP destination router that was previously busy.
<b>l2tp tunnel hello</b>	Sets the number of seconds between sending hello keepalive packets for an L2TP tunnel.

**Table 1** *Commands Available for VPDN Template Configuration (continued)*

<b>Command Name</b>	<b>Description</b>
<b>l2tp tunnel password</b>	Sets the password the router uses to authenticate the tunnel.
<b>l2tp tunnel receive-window</b>	Configures the number of packets in the receive window for the control channel.
<b>l2tp tunnel retransmit initial retries</b>	Configures the number of times after which a router will stop attempting to send the initial control packet for L2TP tunnel establishment to a busy router.
<b>l2tp tunnel retransmit initial timeout</b>	Configures the amount of time that the router waits before resending an initial packet to establish a tunnel.
<b>l2tp tunnel retransmit retries</b>	Configures the number of times that the router attempts to establish a tunnel.
<b>l2tp tunnel retransmit timeout</b>	Configures the amount of time that the router waits before tearing down a tunnel.
<b>l2tp tunnel timeout setup</b>	Configures the amount of time permitted to set up a tunnel.
<b>local name</b>	Specifies a local host name that the tunnel will use to identify itself.
<b>pptp flow-control receive-window</b>	Specifies how many packets the client can send before it must wait for the acknowledgment from the tunnel server.
<b>pptp flow-control static-rtt</b>	Specifies the timeout interval of the tunnel server between sending a packet to the client and receiving a response.
<b>pptp tunnel echo</b>	Specifies the period of idle time on the tunnel that will trigger an echo message from the tunnel server to the client.

**Examples**

The following example shows how to enter VPDN template configuration mode and configure two VPDN parameters in the VPDN template:

```
vpdn-template
 l2tp tunnel busy timeout 65
 l2tp tunnel password 7 tunnel4me
```

The following example shows how to configure a VPDN template called customer1 and apply a group session limit of 50 to all VPDN groups attached to that VPDN template:

```
vpdn-template customer1
 group session-limit 50
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>group session-limit</b>	Specifies the maximum concurrent sessions allowed across all VPDN groups associated with a particular VPDN template.
<b>session-limit</b>	Limits the number of VPDN sessions.
<b>session-limit (VPDN)</b>	Limits the number of sessions that are allowed through a specified VPDN group.
<b>show vpdn session</b>	Displays information about active L2F Protocol tunnel and message identifiers in a VPDN.
<b>source vpdn-template</b>	Configures an individual VPDN group to use system default settings rather than the VPDN template settings for all unspecified parameters.
<b>vpdn-group</b>	Associates a VPDN group to a customer or VPDN profile.
<b>vpdn session-limit</b>	Limits the number of simultaneous VPN sessions that can be established on a router.

## Glossary

**HGW**—home gateway, also known as LNS in L2TP contexts.

**L2F**—Layer 2 Forwarding Protocol. Protocol that supports the creation of secure virtual private dialup networks over the Internet.

**L2TP**—Layer 2 Tunneling protocol. An Internet Engineering Task Force (IETF) standards track protocol defined in RFC 2661 that provides tunneling of PPP. Based upon the best features of L2F and PPTP, L2TP provides an industry-wide interoperable method of implementing VPDN.

**LAC**—L2TP access concentrator. A node that acts as one side of an L2TP tunnel endpoint and is a peer to the L2TP network server (LNS). The LAC is located between an LNS and a remote system and forwards packets to and from each. Packets sent from the LAC to the LNS require tunneling with the L2TP Protocol. The connection from the LAC to the remote system is either local or a PPP link.

**LNS**—L2TP network server. A node that acts as one side of an L2TP tunnel endpoint and is a peer to the L2TP access concentrator (LAC). The LNS is the logical termination point of a PPP session that is being tunneled from the remote system by the LAC. Analogous to the Layer 2 Forwarding (L2F) home gateway (HGW).

**NAS**—network access server, also known as LAC in L2TP context. Cisco platform (or collection of platforms, such as an AccessPath system) that interfaces between the packet world (for example, the Internet) and the circuit world (for example, the PSTN).

**PPPoE**—Point-to-Point Protocol over Ethernet.

**PPTP**—Point-to-Point Tunneling Protocol. RFC 2637 describes the PPTP protocol.

**VPDN**—virtual private dialup network. Also known as virtual private dial network. A VPDN is a network that extends remote access to a private network using a shared infrastructure. VPDNs use Layer 2 tunnel technologies (L2F, L2TP, and PPTP) to extend the Layer 2 and higher parts of the network connection from a remote user across an ISP network to a private network. VPDNs are a cost-effective method of establishing a long distance, point-to-point connection between remote dial users and a private network.

**VRF**—VPN routing and forwarding. A VRF consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what goes into the forwarding table. In general, a VRF includes the routing information that defines a customer VPN site that is attached to a provider edge (PE) router.

**Note**

---

Refer to [Internetworking Terms and Acronyms](#) for terms not included in this glossary.

---



|