



Virtual Private Dialup Network Commands

This chapter describes the commands required to configure virtual private dialup networks. For information about configuring this feature, see the “Configuring Virtual Private Dialup Networks” chapter of the *Dial Solutions Configuration Guide*.

clear vpdn tunnel

To shut down a specified tunnel and all the MIDs within it, use the **clear vpdn tunnel EXEC** command.

clear vpdn tunnel *network-access-server gateway-name*

Syntax Description

<i>network-access-server</i>	Name of the network access server at the far end of the tunnel, probably the point of presence of the public data network or the Internet Service Provider's.
<i>gateway-name</i>	Host name of home gateway at the local end of the tunnel.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2.

This command is used primarily for troubleshooting. You can use the command to force the tunnel to come down without unconfiguring it (the tunnel could be restarted immediately by a user logging in).

Example

The following example clears a tunnel between a network access server called orion and a home gateway called sampson:

```
clear vpdn tunnel orion sampson
```

show vpdn

To display information about active Level 2 Forwarding (L2F) protocol tunnel and Level 2 Forwarding (L2F) message identifiers in a virtual private dialup network, use the **show vpdn** EXEC command.

show vpdn

Syntax Description

This command has no keywords or arguments.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2.

Sample Display

The following is sample output of the **show vpdn** command:

```
Router# show vpdn

Active L2F tunnels
NAS Name      Gateway Name      NAS CLID      Gateway CLID      State
nas           gateway           4             2                 open

L2F MIDs
Name          NAS Name          Interface      MID              State
phil@cisco.com  nas              As7           1                open
sam@cisco.com  nas              As8           2                open
```

Table 125 describes the fields in this sample display.

Table 125 Show VPDN Field Descriptions

Field	Description
Active L2F tunnels	
NAS Name	Host name of the network access server, which is the remote termination point of the tunnel.
Gateway Name	Host name of the home gateway, which is local termination point of the tunnel.
NAS CLID	A number uniquely identifying the VPDN tunnel on the network access server.
Gateway CLID	A number uniquely identifying the VPDN tunnel on the gateway
State	Indicates whether the tunnel is open, opening, closing, or closed.
L2F MIDs	
Name	Username of the person from whom a protocol message was forwarded over the tunnel.
NAS Name	Host name of the network access server.

Table 125 Show VPDN Field Descriptions (Continued)

Field	Description
Interface	Interface from which the protocol message was sent.
MID	A number uniquely identifying this user in this tunnel.
State	Indicates status for the individual user in the tunnel. The states are: opening, open, closed, closing, and waiting_for_tunnel. The waiting_for_tunnel state means that the user connection is waiting until the main tunnel can be brought up before it moves to the opening state.

Related Commands

You can use the master indexes or search online to find documentation of related commands.

- vpdn enable**
- vpdn incoming**
- vpdn outgoing**

vpdn aaa attribute

To specify selected AAA attributes for the AAA server for vpdn tunnel authorization, use the **vpdn aaa attribute** global configuration command.

```
vpdn aaa attribute [nas-ip-address | nas-port]
```

Syntax Description

<i>nas-ip-address</i>	Designates VPDN NAS IP address.
<i>nas-port</i>	Designates VPDN NAS port.

Default

This command is disabled.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2F.

If configured in an environment with an existing AAA server, vpdn tunnel authorization will go through selected AAA servers only.

This command allows the network access server to parse a list of home gateway DNS domain names and addresses sent by an AAA server. The AAA server can store domain names or IP addresses in the following AV pair:

```
cisco-avpair = "lcp:interface-config=ip address 1.1.1.1 255.255.255.255.0",  
cisco-avpair = "lcp:interface-config=ip address bigrouter@excellentinc.com,
```

Examples

The following example lists three suffix delimiters and three prefix delimiters:

```
vpdn domain-delimiter %-@ suffix  
vpdn domain-delimiter #/\ \ prefix
```

This example allows the following host and domain names:

```
cisco.com#houstondrr  
houstondrr@cisco.com
```

Related Commands

tacacs-server directed-request restricted

vpdn aaa override-server

To specify the AAA server for vpdn tunnel authorization, use the **vpdn aaa override-server** global configuration command.

```
vpdn aaa override-server[name | IP]
```

Syntax Description

<i>name</i>	Name of AAA server.
<i>IP</i>	IP address of AAA server.

Default

This command is disabled.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2F.

If configured in an environment with an existing AAA server, vpdn tunnel authorization will go through selected AAA servers only.

Examples

The following example :

```
vpdn aaa override-server 10.10.10.10  
vpdn aaa override-server 12.12.12.12
```

Related Commands

tacacs-server directed-request restricted

vpdn domain-delimiter

To specify the characters to be used to delimit the domain prefix or domain suffix, use the **vpdn domain-delimiter** global configuration command.

```
vpdn domain-delimiter characters [suffix | prefix]
```

Syntax Description

characters

One or more specific characters to be used as suffix or prefix delimiters. Available characters are %, -, @, \, #, and /.

If a backslash (\) is the last delimiter in the command line, enter it as a double backslash (\\).

suffix | **prefix**

Usage of the specified characters.

Default

This command is disabled.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3.

You can enter one **vpdn domain-delimiter** command to list the suffix delimiters and another **vpdn domain-delimiter** command to list the prefix delimiters. However, no character can be both a suffix delimiter and a prefix delimiter.

This command allows the network access server to parse a list of home gateway DNS domain names and addresses sent by an AAA server. The AAA server can store domain names or IP addresses in the following AV pair:

```
cisco-avpair = "lcp:interface-config=ip address 1.1.1.1 255.255.255.255.0",  
cisco-avpair = "lcp:interface-config=ip address bigrouter@excellentinc.com,
```

Examples

The following example lists three suffix delimiters and three prefix delimiters:

```
vpdn domain-delimiter %-@ suffix  
vpdn domain-delimiter #/\ \ prefix
```

This example allows the following host and domain names:

```
cisco.com#houstondrr  
houstondrr@cisco.com
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

vpdn enable
vpdn incoming
vpdn outgoing
vpdn search-order

vpdn enable

To enable virtual private dialup networking on the router and inform the router to look for tunnel definitions in a local database and on a remote authorization server (home gateway), if one is present, use the **vpdn enable** global configuration command.

vpdn enable

Syntax Description

This command has no keywords or arguments.

Default

Disabled

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2.

Note To disable a VPN tunnel, use the **clear vpdn tunnel** command in the EXEC mode. The **no vpdn enable** command does not automatically disable a VPN tunnel.

Example

The following example enables virtual private dialup networking on the router:

```
vpdn enable
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

vpdn incoming

vpdn outgoing

vpdn force-local-chap

To cause the home gateway to issue its own CHAP challenge even if one has already been issued from the network access server, use the **vpdn force-local-chap** global configuration command. To disable the home gateway's issuing its own CHAP challenge, use the **no** form of this command.

vpdn force-local-chap
no vpdn force-local-chap

Syntax Description

This command has no arguments or keywords.

Default

The home gateway does not issue its own CHAP challenge.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2.

Example

The following example configures a virtual template interface on the home gateway and then enables VPDN and forces the home gateway to issue its own CHAP challenge.

```
interface virtual-template 1
ip unnumbered ethernet 0
encapsulation ppp
ppp authentication chap
!
vpdn enable
vpdn incoming world12 troll virtual-template 1
vpdn force-local-chap
```

vpdn incoming

To specify the local name to use for authenticating and the virtual template to use for building interfaces for incoming connections when a Level 2 Forwarding (tunnel) connection is requested from a certain remote host, use the **vpdn incoming** global configuration command.

```
vpdn incoming remote-name local-name virtual-template number
```

Syntax Description

<i>remote-name</i>	Case-sensitive name of the remote host requesting the connection.
<i>local-name</i>	Case-sensitive local name to use when authenticating back to the remote host.
virtual-template <i>number</i>	Virtual template to use for building interfaces for incoming calls.

Default

Disabled. No host name, IP address, or local name for authentication are provided.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2.

The *remote-name* and *local-name* arguments are case sensitive.

This command is usually used on a home gateway, not on the network access server in the ISP or public data network.

Example

The following partial example specifies use of local host `go_blue` and virtual template interface 6 for connections with remote host `dallas_wan`:

```
vpdn incoming dallas_wan go_blue virtual-template 6
```

vpdn local-authentication

To enable local authentication of users on the network access server before the connection is forwarded to the home gateway, use the **vpdn local-authentication** global configuration command. To reset the network access server to the default in which local authentication is disabled, use the **no** form of this command.

vpdn local-authentication
no vpdn local-authentication

Syntax Description

This command has no arguments and keywords.

Default

This command is disabled.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3.

Example

In the following example, the network access server is configured to select tunnels based on the dialed number of incoming calls and to authenticate users locally:

```
vpdn enable
vpdn outgoing dnis 4592367 spartan ip 172.34.16.244
vpdn local-authentication
```

Related Commands

You can use the master indexes or search online for documentation of related commands.

vpdn enable
vpdn outgoing

vpdn outgoing

To specify use of Dialed Number Information Service (DNIS) or use of a domain name when selecting a tunnel for forwarding traffic to the remote host (the home gateway) on a virtual private dialup network, use the **vpdn outgoing** global configuration command.

```
vpdn outgoing word | dnis dialed-number
```

Syntax Description

word	Case-sensitive name of the gateway domain for forwarding traffic.
dnis <i>dialed-number</i>	Dialed number to be used for selecting a specific tunnel for forwarding traffic to a home gateway.

Default

Disabled. No remote names and local names are defined.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2

The **word** argument is case sensitive.

This command is usually used on a network access server, not on a home gateway.

When use of the Dialed Number Information Service is enabled and a dialed number is provided, the network service provider can use the dialed number to select a specific tunnel destination.

The domain name can be used to choose a tunnel destination. For example, if a user dials in as "joe@company-a.com," then matching on "company-a.com," a tunnel destination can be chosen.

If both DNIS information and a CHAP or PAP name map to a valid tunnel, the DNIS information is used.

If TACACS+ is used to get tunnel information, the string "dnis:" is prepended to the phone number before attempting to look up the information in AAA.

Examples

The following example selects a tunnel destination based on the domain name:

```
vpdn outgoing chicago-main go-blue
```

The following example selects a tunnel destination based on the use of DNIS and a specific dialed number:

```
vpdn outgoing dnis 2387765 gocardinal
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

vpdn enable

vpdn incoming

vpdn search-order

To specify how the service provider's network access server is to perform VPDN tunnel authorization searches, use the **vpdn search-order** global configuration command. To remove a prior specification, use the **no** form of the command.

```
vpdn search-order { dnis domain | domain dnis | domain | dnis }  
no vpdn search-order
```

Syntax Description

dnis domain	Search first on the Dialed Number Information Service (DNIS) information provided on ISDN lines and then search on the domain name.
domain dnis	Search first on the domain name and then search on the DNIS information.
domain	Search on the domain name only.
dnis	Search on the DNIS information only.

Default

When this command is not used, the default is to search first on the Dialed Number Information Service (DNIS) information provided on ISDN lines and then search on the domain name. This is equivalent to using the **vpdn search-order dnis domain** command.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3.

VPDN authorization searches are performed only as specified.

The configuration shows the **vpdn search-order** command setting only if the command is explicitly configured.

Example

The following example configures a network access server to select a tunnel destination based on the use of DNIS and a specific dialed number and to perform tunnel authorization searches based on the DNIS information only.

```
vpdn enable  
vpdn outgoing dnis 2387765 gocardinal ip 170.16.44.56  
vpdn search-order dnis
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

vpdn outgoing

vpdn source-ip

To set the source IP address of the network access server, use the **vpdn source-ip** global configuration command.

```
vpdn source-ip address
```

Syntax Description

address IP address of the network access server.

Default

This command is disabled. No default IP address is provided.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3.

One source IP address is configured on the network access server. The source IP address is configured per network access server, not per domain.

Example

This example enables VPDN on the network access server and sets an IP source address of 171.4.48.3.

```
vpdn enable  
vpdn source-ip 171.4.48.3
```

Related Commands

You can use the master indexes or search online for documentation of related commands.

vpdn enable

