



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 history failure

To clear the content of the failure history table, use the **clear vpdn history failure** EXEC command.

clear vpdn history failure

Syntax Description

This command has no arguments or keywords.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3 T.

Example

The following example clears the content of the failure history table:

```
clear vpdn history failure
```

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 138 describes the fields in this sample display.

Table 138 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 138 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 history failure

show vpdn history failure

To show the content of the failure history table, use the **show vpdn history failure** with the optional username keyword EXEC command.

```
show vpdn history failure [username]
```

Syntax Description

username (Optional) Specifies the username. The specified username helps to display only the entries mapped to that particular user.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3 T.

If a username is specified, only the entries mapped to that username are displayed; when the username is not specified, the whole table is displayed.

Sample Display

The following is a sample output from the **show vpdn history failure** command, which displays the failure history table for a specific user:

```
router> show vpdn history failure
Table size: 20
Number of entries in table: 1

User: jcchan@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
```

Table 139 describes the fields shown in the sample output.

Table 139 Show VPDN History Failure Field Descriptions

Field	Description
Table size	Configurable VPDN history table size.
Number of entries in table	Number of entries currently in the history table.
User	Username for the entry displayed.
MID	VPDN user session ID that correlates to the logged event. The MID is a unique ID per user session.
NAS	Network access server identity.
IP address	IP address of the NAS or home gateway (HGW).
CLID	Tunnel endpoint for the NAS and HGW.

Table 139 Show VPDN History Failure Field Descriptions (continued)

Field	Description
Gateway	HGW end of the VPDN tunnel.
Log time	The event logged time.
Error repeat count	Number of times a failure entry has been logged under a specific user. Only one log entry is allowed per user and is unique to its MID, with the older one being overwritten.
Failure type	Description of failure.
Failure reason	Reason for failure.

Related Commands

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

clear vpdn history failure

vpdn history failure

vpngn aaa attribute

To enable reporting of network access server (NAS) authentication, authorization, and accounting (AAA) attributes related to a virtual private dialup network (VPDN) to the AAA server, use the **vpngn aaa attribute** global configuration command. To disable reporting of AAA attributes related to VPDN, use the **no** form of this command.

```
vpngn aaa attribute { nas-ip-address vpngn-nas | nas-port vpngn-nas }
```

```
no vpngn aaa attribute { nas-ip-address vpngn-nas | nas-port }
```

Syntax Description

nas-ip-address vpngn-nas	Enable reporting of the VPDN NAS IP address to the AAA server..
nas-port vpngn-nas	Enable reporting of the VPDN NAS port to the AAA server.

Default

AAA attributes are not reported to the AAA server.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3NA.

This command can be used with RADIUS or TACACS+, and is applicable only on the VPDN tunnel server.

Examples

The following example configures VPDN on a tunnel server and enables reporting of VPDN AAA attributes to the AAA server:

```
vpngn enable
vpngn-group 1
  accept-dialin
  protocol any
  virtual-template 1
!
  terminate-from hostname nas1
  local name ts1
!
vpngn aaa attribute nas-ip-address vpngn-nas
vpngn aaa attribute nas-port vpngn-nas
```

Related Commands

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

aaa new-model
vpngn enable

vpdn aaa override-server

To specify an authentication, authorization, and accounting (AAA) server to be used for virtual private dialup network (VPDN) tunnel authorization other than the default AAA server, use the **vpdn aaa override-server** global configuration command. To return to the default setting, use the **no** form of this command.

```
vpdn aaa override-server {aaa-server-ip-address | aaa-server-name}
```

```
no vpdn aaa override-server {aaa-server-ip-address | aaa-server-name}
```

Syntax Description

<i>aaa-server-ip-address</i>	The IP address of the AAA server to be used for tunnel authorization.
<i>aaa-server-name</i>	The name of the AAA server to be used for tunnel authorization.

Default

If the AAA server is not specified, the default AAA server configured for network authorization is used.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2F.

This command can be used with RADIUS or TACACS+, and is applicable only on the VPDN network access server (NAS). Configuring this command restricts tunnel authorization to the specified AAA servers only. This command can be used to specify multiple AAA servers.

For TACACS+ configuration, the **tacacs-server directed-request** command must be configured using the **restricted** keyword, or authorization will continue with all configured TACACS+ servers.

Examples

The following example enables AAA attributes and specifies the AAA server to be used for VPDN tunnel authorization:

```
aaa new-model
aaa authorization network default group radius
vpdn aaa override-server 10.1.1.1
vpdn enable
radius-server host 10.1.1.2 auth-port 1645 acct-port 1646
radius-server key Secret
```

Related Commands

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

aaa new-model
tacacs-server directed-request
vpdn enable

vpng domain-delimiter

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

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

Syntax Description

<i>characters</i>	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	(Optional) 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 **vpng domain-delimiter** command to list the suffix delimiters and another **vpng 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:

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

This example allows the following host and domain names:

```
cisco.com#houstonddr
houstonddr@cisco.com
```

Related Commands

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

vpdn enable
vpdn history failure
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 command **clear vpn tunnel** in EXEC mode. The command **no vdpn enable** 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 history failure

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 history failure

To enable logging of virtual private dialup network (VPDN) failures to the history failure table or to set the failure history table size, use the **vpdn history failure** command in global configuration mode. To disable logging of VPDN history failures or to restore the default table size, use the **no** form of this command.

```
vpdn history failure [table-size entries]
```

```
no vpdn history failure [table-size]
```

Syntax Description

table-size (Optional) Sets the number of entries in the history failure table.
entries Valid entries range from 20 to 50.

Default

VPDN failures are logged by default.
table size: 20 entries

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3 T.

Logging of VPDN failure events is enabled by default. You can disable the logging of VPDN failure events by issuing the **no vpdn history failure** command.

The logging of a failure event to the history table is triggered by event logging by the syslog facility. The syslog facility creates a failure history table entry, which keeps records of failure events. The table starts with 20 entries, and the size of the table can be expanded to a maximum of 50 entries using the **vpdn history failure table-size** *entries* command. You may configure the **vpdn history failure table-size** *entries* command only if VPDN failure event logging is enabled.

All failure entries for the user 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 table size, the oldest record is deleted and a new entry is added.

Example

The following example disables logging of VPDN failures to the history failure table:

```
no vpdn history failure
```

The following example enables logging of VPDN failures to the history table and sets the history failure table size to 40 entries:

```
vpdn history failure  
vpdn history failure table-size 40
```

Related Commands

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

show vpdn history failure

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 (the network access server) requesting the connection.
<i>local-name</i>	Case-sensitive local name (of the home gateway) 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 logging

To enable the logging of VPDN events, use the **vpdn logging** global configuration command. To disable the logging of VPDN events, use the **no** form of this command.

vpdn logging [local | remote]
no vpdn logging [local | remote]

Syntax Description

local	(Optional) Log VPDN events locally.
remote	(Optional) Log VPDN events to a remote tunnel endpoint.

Default

Enabled

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3 T.

This command logs VPDN events. By default, VPDN logging is enabled; therefore, if you wish to disable VPDN event logging, you must explicitly configure the router using the **no** form of the command.

Example

The default behavior is to log VPDN events; however, if you wish to reenble the feature after removal, the following example shows how to reenble VPDN logging locally:

```
vpdn logging local
```

Related Commands

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

vpdn history failure

vpdn multihop

To enable virtual private dialup network (VPDN) multihop, use the **vpdn multihop** global configuration command. To disable VPDN multihop capability, use the **no** form of this command.

vpdn multihop

no vpdn multihop

Syntax Description

This command has no arguments or keywords.

Default

Multihop is not enabled.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3(5)T.

The Cisco Multihop VPDN feature allows you to perform Multichassis Multilink Point-to-Point Protocol (MMP) on a home gateway (HGW) or Layer 2 Tunneling Protocol (L2TP) network server (LNS) in a VPDN scenario. This feature allows sharing tunnel resources between the HGW and LNS routers, and the possibility to offload by default to another router in the network.

The VPDN multihop feature also allows a router configured as a tunnel switch to terminate tunnels from Layer 2 access concentrators (LACs) and forward the sessions through up to four newly established L2TP tunnels. The tunnels are selected using client-supplied matching criteria configured by the **vpdn search-order** global configuration command.

Before using the **vpdn multihop** command, refer to the *Dial Solutions Configuration Guide* to learn more about Multilink PPP and MMP.

Example

The following example shows a configuration where a packet traverses a VPDN tunnel over a service provider link, and then a second tunnel by traversing a hop between home gateways on the corporate network. The bundle owner is Home-Gateway1 and the stack group peer, Home-Gateway2, is specified as a peer (10.10.1.2).

```
vpdn multihop
username stack password hellothere
multilink virtual-template 1

sgbp group stack
sgbp member Home-Gateway2 10.10.1.2

interface virtual-template 1
ip unnumbered e0
ppp multilink
ppp auth chap
```

Related Commands

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

vpdn enable
vpdn search-order

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 history failure

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

