A through K

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

aaa accounting nested

To specify that NETWORK records be generated, or nested, within EXEC start and stop records for PPP users who start EXEC terminal sessions, use the **aaa accounting nested** command in global configuration mode. To allow the sending of records for users with a NULL username, use the **no** form of this command.

aaa accounting nested [**suppress stop**]

no aaa accounting nested [**suppress stop**]

Syntax Description

suppress stop	(Optional) Prevents sending a multiple set of records (one from EXEC and one from PPP) for the same client.

Command Default

Disabled

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	The **suppress** and the **stop** keywords were added.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **aaa accounting nested** command when you want to specify that NETWORK records be nested within EXEC start and stop records, such as for PPP users who start EXEC terminal sessions. In some cases, such as billing customers for specific services, it can be desirable to keep NETWORK start and stop records together, essentially nesting them within the framework of the EXEC start and stop messages. For example, if you dial in using PPP, you can create the following records: EXEC-start, NETWORK-start, EXEC-stop, and NETWORK-stop. By using the **aaa accounting nested** command to generate accounting records, NETWORK-stop records follow NETWORK-start messages: EXEC-start, NETWORK-start, NETWORK-stop, EXEC-stop.

Use the **aaa accounting nested suppress stop** command to suppress the sending of EXEC-stop accounting records and to send only PPP accounting records.

Examples

The following example enables nesting of NETWORK accounting records for user sessions:

```
Router(config)# aaa accounting nested
```

The following example disables nesting of EXEC accounting records for user sessions:

```
Router(config)# aaa accounting nested suppress stop
```

accept-dialin

To create an accept dial-in virtual private dialup network (VPDN) subgroup that configures a tunnel server to accept requests from a network access server (NAS) to tunnel dial-in calls, and to enter accept dial-in VPDN subgroup configuration mode, use the **accept-dialin** command in VPDN group configuration mode. To remove the accept dial-in VPDN subgroup configuration from a VPDN group, use the **no** form of this command.

accept-dialin

no accept-dialin

Syntax Description

This command has no arguments or keywords.

Command Default

No accept dial-in VPDN subgroups are configured.

Command Modes

VPDN group configuration (config-vpdn)

Command History

Release	Modification
11.3(5)AA	This command was introduced and replaced the **vpdn incoming** command used in Cisco IOS Release 11.3.
12.0(1)T	This command was integrated into Cisco IOS Release 12.0(1)T and implemented on additional router and access server platforms.
12.0(5)T	The original keywords and arguments were removed and made into separate **accept-dialin** subgroup commands.
12.1(1)T	This command was enhanced to support dial-in Point-to-Point Protocol over Ethernet (PPPoE) calls.

Usage Guidelines

Use the **accept-dialin** command on a tunnel server to configure a VPDN group to accept requests to establish dial-in VPDN tunnels from a NAS. Once the tunnel server accepts the request from a NAS, it uses the specified virtual template to clone new virtual access interfaces.

To configure a VPDN group to accept dial-in calls, you must also configure these commands:

- The **protocol** command from accept dial-in VPDN subgroup configuration mode

- The **virtual-template** command from accept dial-in VPDN subgroup configuration mode (configuring this command is not required if the virtual access interface is not going to be cloned when a user connects)
- The **terminate-from** command in VPDN group configuration mode

Note If you create a VPDN group without configuring a **terminate-from** command, a default VPDN group is automatically enabled. Incoming tunnel requests from any hostname use the attributes specified in the default VPDN group unless a specific VPDN group is configured with a **terminate-from** command using that hostname.

Typically, you need one VPDN group for each NAS that will be tunneling to the tunnel server. For a tunnel server that services many NASs, the configuration can become cumbersome. If all NASs share the same tunnel attributes, you can simplify the configuration by using the default VPDN group configuration, or by creating a VPDN default group template using the **vpdn-template** command.

The tunnel server can also be configured to request the establishment of Layer 2 Tunnel Protocol (L2TP) dial-out VPDN tunnels to a NAS by using the **request-dialout** command. Dial-in and dial-out calls can use the same L2TP tunnel.

Examples

The following example enables the tunnel server to accept Layer 2 Forwarding (L2F) tunnels from a NAS named router23. A virtual-access interface is cloned from virtual-template 1.

```
Router(config)# vpdn-group 1
Router(config-vpdn)# accept-dialin
Router(config-vpdn-acc-in)# protocol l2f
Router(config-vpdn-acc-in)# virtual-template 1
!
Router(config-vpdn)# terminate-from hostname router23
```

The following example configures the router so that tunnels requested by the NAS named router16 are created with the tunnel attributes specified by VPDN group 1, while any other incoming L2TP tunnel request use the settings configured in the default VPDN group, VPDN group 2:

```
Router(config)# vpdn-group 1
Router(config-vpdn)# accept-dialin
Router(config-vpdn-acc-in)# protocol l2tp
Router(config-vpdn-acc-in)# virtual-template 2
!
Router(config-vpdn)# terminate-from hostname router16
Router(config)# vpdn-group 2
! Default L2TP VPDN group
Router(config-vpdn)# accept-dialin
Router(config-vpdn-acc-in)# protocol l2tp
Router(config-vpdn-acc-in)# virtual-template 3
```

Related Commands

Command	Description
protocol (VPDN)	Specifies the tunneling protocol that a VPDN subgroup will use.

Command	Description
request-dialin	Creates a request dial-in VPDN subgroup that configures a NAS to request the establishment of a dial-in tunnel to a tunnel server, and enters request dial-in VPDN subgroup configuration mode.
request-dialout	Creates a request dial-out VPDN subgroup that configures a tunnel server to request the establishment of dial-out L2TP tunnels to a NAS, and enters request dial-out VPDN subgroup configuration mode.
terminate-from	Specifies the hostname of the remote LAC or LNS that will be required when accepting a VPDN tunnel.
virtual-template	Specifies which virtual template is used to clone virtual-access interfaces.
vpdn-group	Associates a VPDN group to a customer or VPDN profile.
vpdn-template	Enters VPDN template configuration mode to configure a VPDN template.

accept-dialout

To create an accept dial-out virtual private dialup network (VPDN) subgroup that configures a network access server (NAS) to accept requests from a tunnel server to tunnel Layer 2 Tunneling Protocol (L2TP) dial-out calls, and to enter accept dial-out VPDN subgroup configuration mode, use the **accept-dialout** command in VPDN group configuration mode. To remove the accept dial-out VPDN subgroup configuration from the VPDN group, use the **no** form of this command.

accept-dialout

no accept-dialout

Syntax Description

This command has no arguments or keywords.

Command Default

No accept dial-out VPDN subgroups are configured.

Command Modes

VPDN group configuration (config-vpdn)

Command History

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

Usage Guidelines

Use the **accept-dialout** command on a NAS to configure a VPDN group to accept requests for dial-out VPDN tunnels from a tunnel server. L2TP is the only tunneling protocol that can be used for dial-out VPDN tunnels.

For a VPDN group to accept dial-out calls, you must also configure these commands:

- The **terminate-from** command in VPDN group configuration mode
- The **protocol l2tp** command in accept dial-out VPDN subgroup configuration mode
- The **dialer** command in accept dial-out VPDN subgroup configuration mode
- The **dialer aaa** command in dialer interface configuration mode

The NAS can also be configured to request the establishment of dial-in VPDN tunnels to a tunnel server by using the **request-dialin** command. Dial-in and dial-out calls can use the same L2TP tunnel.

Examples

The following example configures a VPDN group on the NAS to accept L2TP tunnels for dial-out calls from the tunnel server TS23 using dialer 2 as its dialing resource:

```
Router(config)# vpdn-group 1
Router(config-vpdn)# accept-dialout
```

```
Router(config-vpdn-acc-ou)# protocol l2tp
Router(config-vpdn-acc-ou)# dialer 2
!
Router(config-vpdn)# terminate-from hostname TS23
!
Router(config)# interface Dialer2
Router(config-if)# ip unnumbered Ethernet0
Router(config-if)# encapsulation ppp
Router(config-if)# dialer in-band
Router(config-if)# dialer aaa
Router(config-if)# dialer-group 1
Router(config-if)# ppp authentication chap
```

Related Commands

Command	Description
dialer	Specifies the dialer interface that an accept-dialout VPDN subgroup uses to dial out calls.
dialer aaa	Allows a dialer to access the AAA server for dialing information.
dialer vpdn	Enables a Dialer Profile or DDR dialer to use L2TP dial-out.
protocol (VPDN)	Specifies the tunneling protocol that a VPDN subgroup will use.
request-dialin	Creates a request dial-in VPDN subgroup that configures a NAS to request the establishment of a dial-in tunnel to a tunnel server, and enters request dial-in VPDN subgroup configuration mode.
request-dialout	Creates a request dial-out VPDN subgroup that configures a tunnel server to request the establishment of dial-out L2TP tunnels to a NAS, and enters request dial-out VPDN subgroup configuration mode.
terminate-from	Specifies the hostname of the remote router that is required when accepting a VPDN tunnel.

authen-before-forward

To configure a network access server (NAS) to request authentication of a complete username before making a forwarding decision for dial-in Layer 2 Tunnel Protocol (L2TP) or Layer 2 Forwarding (L2F) tunnels belonging to a virtual private dialup network (VPDN) group, use the **authen-before-forward** command in VPDN group configuration mode. To disable this configuration, use the **no** form of this command.

authen-before-forward

no authen-before-forward

Syntax Description

This command has no arguments or keywords.

Command Default

L2TP or L2F tunnels are forwarded to the tunnel server without first requesting authentication of the complete username.

Command Modes

VPDN group configuration (config-vpdn)

Command History

Release	Modification
11.3(9) AA	This command was introduced.
12.0(5)T	This command was integrated into Cisco IOS Release 12.0(5)T and was modified to be available only when the request-dialin VPDN subgroup is enabled.

Usage Guidelines

To configure the NAS to perform authentication of dial-in L2TP or L2F sessions belonging to a specific VPDN group before the sessions are forwarded to the tunnel server, use the **authen-before-forward** command in VPDN group configuration mode.

To configure the NAS to perform authentication of all dial-in L2TP or L2F sessions before the sessions are forwarded to the tunnel server, configure the **vpdn authen-before-forward** command in global configuration mode.

You must configure a request dial-in VPDN subgroup by issuing the **request-dialin** command before you can configure the **authen-before-forward** command. Removing the **request-dialin** configuration removes the **authen-before-forward** command configuration from the VPDN group.

Enabling the **authen-before-forward** command instructs the NAS to authenticate the complete username before making a forwarding decision based on the domain portion of the username. A user may be forwarded or terminated locally depending on the information contained in the users RADIUS profile.

Users with forwarding information in their RADIUS profile are forwarded based on that information. Users without forwarding information in their RADIUS profile are either forwarded or terminated locally based on the Service-Type in their RADIUS profile. The relationship between forwarding decisions and the information contained in the users RADIUS profile is summarized in the table below.

Table 1 Forwarding Decisions Based on RADIUS Profile Attributes

Forwarding Information Is	Service-Type Is Outbound	Service-Type Is Not Outbound
Present in RADIUS profile	Forward User	Forward User
Absent from RADIUS profile	Check Domain	Terminate Locally

Examples

The following example configures an L2F request dial-in VPDN subgroup that sends the entire username to the authentication, authorization, and accounting (AAA) server when a user dials in with a username that includes the domain cisco.com:

```
vpdn-group 1
 request-dialin
  protocol l2f
  domain cisco.com
 initiate-to ip 10.0.0.1
 local name router32
 authen-before-forward
```

Related Commands

Command	Description
ppp multilink	Enables MLP on an interface and, optionally, enables dynamic bandwidth allocation.
request-dialin	Configures a LAC to request L2F or L2TP tunnels to an LNS and create a request-dialin VPDN subgroup, and specifies a dial-in L2F or L2TP tunnel to a remote peer if a dial-in request is received for a specified domain or DNIS.
vpdn authen-before-forward	Configures a NAS to request authentication of a complete username before making a forwarding decision for all dial-in L2TP or L2F tunnels.

authenticate (control policy-map class)

To initiate an authentication request for an Intelligent Services Gateway (ISG) subscriber session, use the **authenticate** command in control policy-map class configuration mode. To remove an authentication request for an ISG subscriber session, use the **no** form of this command.

action-number **authenticate** [**variable** *varname*] [**aaa list**{*list-name* | **default**}]

no *action-number* **authenticate** [**variable** *varname*] [**aaa list**{*list-name* | **default**}]

Syntax Description

action-number	Number of the action. Actions are executed sequentially within the policy rule.
variable	(Optional) Authenticates using the contents of the *varname*value instead of the unauthenticated username. If you do not specify an **aaa list**, the default AAA authentication list is used.
varname	Specifies that user authentication will be performed on the contents of the *varname* value, if present.
aaa list	(Optional) Specifies that authentication will be performed using an authentication, authorization, and accounting (AAA) method list.
list-name	Specifies the AAA method list to which the authentication request will be sent.
default	Specifies the default AAA method list to which the authentication request will be sent.

Command Default

The control policy will not initiate authentication.

Command Modes

Control policy-map class configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(31)SB2	The **variable** keyword and *varname* argument were added.

Usage Guidelines

The **authenticate** command configures an action in a control policy map.

Control policies define the actions the system will take in response to specified events and conditions. A control policy map is used to configure an ISG control policy. A control policy is made of one or more control policy rules. A control policy rule is an association of a control class and one or more actions. The control class defines the conditions that must be met before the actions will be executed. The actions are numbered and executed sequentially within the policy rule.

Note that if you specify the default method list, the default list will not appear in the output of the **show running-config** command. For example, if you configure the following command:

```
Router(config-control-policymap-class-control)# 1 authenticate aaa list default
```

the following will display in the output for the **show running-config** command:

```
1 authenticate
```

Named method lists will display in the **show running-config** command output.

Examples

The following example shows an ISG configured to initiate an authentication request upon account logon. The authentication request will be sent to the AAA method list called AUTH-LIST.

```
policy-map type control LOGIN
 class type control always event account-logon
  1 authenticate aaa list AUTH-LIST
  2 service-policy type service unapply BLIND-RDT
```

The following example shows the policy map configured to initiate an authentication request using a name stored in the variable NEWNAME, instead of unauthenticated-username, using the AAA list EXAMPLE. The authenticate statement is shown in bold:

```
policy-map type control REPLACE_WITH_example.com
 class type control always event session-start
  1 collect identifier unauthenticated-username
  2 set NEWNAME identifier unauthenticated-username
  3 substitute NEWNAME “(.*@).*” “\1example.com”
  4 authenticate variable NEWNAME aaa list EXAMPLE
  5 service-policy type service name example
policy-map type service abc
 service vpdn group 1
bba-group pppoe global
 virtual-template 1
!
interface Virtual-Template1
 service-policy type control REPLACE_WITH_example.com
```

Related Commands

Command	Description
class type control	Specifies a control class for which actions may be configured in an ISG control policy map.
policy-map type control	Creates or modifies a control policy map, which defines an ISG control policy.
set variable	Creates a temporary memory to hold the value of identifier types received by the policy manager.

Command	Description
substitute	Matches the contents, stored in temporary memory of identifier types received by the policy manager, against a specified *matching pattern*and performs the substitution defined in a *rewrite pattern.*

backup

To configure an IP backup endpoint address, enter the **backup** command in VPDN group configuration mode. To remove this function, use the **no** form of this command.

backup ip *ip-address* [**limit** *number* [**priority** *number*]]

no backup ip *ip-address* [**limit** *number* [**priority** *number*]]

Syntax Description

ip *ip-address*	IP address of the HGW/LNS at the other end of the tunnel. This is the IP endpoint at the end of the tunnel, which is an HGW/LNS router.
limit *number*	(Optional) Limits sessions per backup. The range is 0 to 32767. The default is no limit set.
priority *number*	(Optional) Priority level. Loadsharing is priority 1. The range is 2 to 32,767. The highest priority is 2, which is the first home gateway router to receive backup traffic. The lowest priority is 32,767. The priority group is used to support multiple levels of loadsharing and backup. The default is the lowest priority.

Command Default

No default behavior or values. This function is used only if it is configured.

Command Modes

VPDN group configuration (config-vpdn)

Command History

Release	Modification
12.0(4)XI	This command was introduced on the following platforms only: Cisco AS5200 and Cisco AS5300.

Usage Guidelines

Use the **backup** VPDN group configuration command to configure an IP backup endpoint address.

Examples

The following examples show that the **backup** command is not available in the command-line interface until you enter the **request-dialin** command:

```
Router(config)# vpdn-group customer1-vpdngroup
```

```
Router(config-vpdn)# ?
VPDN group configuration commands:
  accept-dialin    VPDN accept-dialin group configuration
  accept-dialout   VPDN accept-dialout group configuration
  default          Set a command to its defaults
  description      Description for this VPDN group
  exit             Exit from VPDN group configuration mode
  ip               IP settings for tunnel
  no               Negate a command or set its defaults
  request-dialin   VPDN request-dialin group configuration
  request-dialout  VPDN request-dialout group configuration
  source-ip        Set source IP address for this vpdn-group
Router(config-vpdn)# request-dialin l2tp ip 10.2.2.2 domain customerx
Router(config-vpdn)#?
VPDN group configuration commands:
  backup            Add backup address
  default           Set a command to its defaults
  dnis              Accept a DNIS tunnel
  domain            Accept a domain tunnel
  exit              Exit from VPDN group configuration mode
  force-local-chap  Force a CHAP challenge to be instigated locally
  l2tp              L2TP specific commands
  lcp               LCP specific commands
  loadsharing       Add loadsharing address
  local             local information, like name
  multilink         Configure limits for Multilink
  no                Negate a command or set its defaults
  request           Request to open a tunnel
```

The following example shows an IP backup endpoint address of 10.1.1.1 configured with a backup session limit of 5:

```
Router(config-vpdn)# backup ip 10.1.1.1 limit 5
```

Related Commands

Command	Description
request-dialin	Configures a LAC to request L2F or L2TP tunnels to an LNS and create a request-dialin VPDN subgroup, and specifies a dial-in L2F or L2TP tunnel to a remote peer if a dial-in request is received for a specified domain or DNIS.

clear l2tp

To clear Layer 2 Tunnel Protocol (L2TP) entities, use the **clear l2tp** command in privileged EXEC mode.

clear l2tp {**all** | **counters** | **l2tp-class** *class-name* | **local ip** *ip-address* | **remote ip** *ip-address* | **tunnel id** *tunnel-id*}

Syntax Description

all	Clears all tunnels.
counters	Clears L2TP counters.
l2tp-class *class-name*	Clears all L2TP tunnels by L2TP class name.
local ip *ip-address*	Clears all respective tunnels associated with the local IP address.
remote ip *ip-address*	Clears all respective tunnels associated with the remote IP address.
tunnel id *tunnel-id*	Clears the specified L2TP tunnel. The range is 1 to 4294967295.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(11)T	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Examples

The following example shows how to clear all tunnels:

```
Router# clear l2tp counters all
```

The following example shows how to clear all tunnels associated with the IP address 10.1.1.1:

```
Router# clear l2tp counters local ip 10.1.1.1
```

This example shows the syslog messages that are displayed at both ends of the tunnel when the **clear l2tp all** command is entered at the LAC:

```
Router-LAC# clear l2tp all
```

```
00:01:28: %VPDN-6-CLOSED: L2TP LAC LAC closed  user user@surf1.org; Result 3, Error 6,
Admin Action
00:01:28: %VPDN-6-CLOSED: L2TP LAC closed tunnel  ; Result 1, Error 6, Admin Action
Router-LAC#
Router-LNS#
00:01:27: %VPDN-6-CLOSED: L2TP LAC closed tunnel  ; Result 1, Error 6, Admin Action
00:01:27: %VPDN-6-CLOSED: L2TP LAC LAC closed Vi2.1 user user@surf1.org; Result 3, Error
6, Admin Action
Router-LNS#
```

This example shows the syslog messages that are displayed at both ends of the tunnel when the **clear l2tp all** command is entered at the LNS:

```
Router-LNS# clear l2tp all
00:02:02: %VPDN-6-CLOSED: L2TP LNS LNS closed Vi2.1 user user@surf1.org; Result 3, Error
6, Admin Action
00:02:02: %VPDN-6-CLOSED: L2TP LNS closed tunnel  ; Result 1, Error 6, Admin Action
Router-LNS#
Router-LAC#
00:02:04: %VPDN-6-CLOSED: L2TP LNS closed tunnel  ; Result 1, Error 6, Admin Action
00:02:04: %VPDN-6-CLOSED: L2TP LNS LNS closed  user user@surf1.org; Result 3, Error 6,
Admin Action
Router-LAC#
```

Related Commands

Command	Description
show l2tp counters	Displays information about L2TP counters and tunnel statistics.
show l2tp session	Displays information about L2TP sessions.
show l2tp tunnel	Displays details about L2TP tunnels.

clear l2tp counters session

To clear Layer 2 Tunnel Protocol (L2TP) session counters associated with a particular subset of sessions, use the **clear l2tp counters session** command in privileged EXEC mode.

clear lt2tp counters session [**fsm** {**event** [**icrq** | **manual** | **ocrq**] | **ip-addr** *ip-address* | **state transition**[**icrq** | **manual** | **ocrq**] | **tunnel**{**id***local-id* [*local-session-id*] | **remote-name** *remote-name local-name* | **username** *username* | **vcid** *vcid*}}]

Syntax Description

fsm	(Optional) Clears finite state machine counters.
event [**icrq** | **manual** | **ocrq**]	(Optional) Clears the specified state machine event counter: • **icrq** --Incoming Call Request (ICRQ), Incoming Call Reply (ICRP), and Incoming Call Connected (ICCN) dial-in state-machine-related counters. • **manual** --Manual session state-machine-related counters. • **ocrq** --Outgoing Call Request (OCRQ), Outgoing Call Reply (OCRP), and Outgoing Call Connected (OCCN) dial-out state-machine-related counters.
ip-addr *ip-address*	(Optional) Clears L2TP session counters for sessions associated with a particular peer IP address.
state transition [**icrq** | **manual** | **ocrq**]	(Optional) Clears the specified state machine transition counter: • **icrq** --Incoming Call Request (ICRQ), Incoming Call Reply (ICRP), and Incoming Call Connected (ICCN) dial-in state-machine-related counters. • **manual** --Manual session state-machine-related counters. • **ocrq** --Outgoing Call Request (OCRQ), Outgoing Call Reply (OCRP), and Outgoing Call Connected (OCCN) dial-out state-machine-related counters.
tunnel	(Optional) Clears L2TP session counters for sessions associated with a particular tunnel.

id *local-id* [*local-session-id*]	(Optional) Clears the tunnel L2TP session counters associated with the specified local tunnel ID, and optionally the local session ID. The range for the local tunnel and the local session IDs is 1 to 4294967295.
remote-name *remote-name local-name*	(Optional) Clears the tunnel L2TP session counters associated with the specified remote tunnel name and local tunnel name.
username *username*	(Optional) Clears the L2TP session counters for the sessions associated with a particular username.
vcid *vcid*	(Optional) Clears that L2TP session counters for the sessions associated with a particular virtual circuit ID (VCID). The range is 1 to 4294967295.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(11)T	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Examples

The following example shows how to clear the session counters for only those sessions associated with the peer at IP address 10.1.1.1:

```
Router# clear l2tp counters session ip-addr 10.1.1.1
```

Related Commands

Command	Description
show l2tp counters	Displays information about L2TP counters and tunnel statistics.
show l2tp session	Displays information about L2TP sessions.
show l2tp tunnel	Displays details about L2TP tunnels.

clear l2tp counters tunnel

To clear Layer 2 Tunnel Protocol (L2TP) tunnel counters, use the **clear l2tp counters tunnel** command in privileged EXEC mode.

clear l2tp counters tunnel [**authentication** | **id** *local-id*]

Syntax Description

authentication	(Optional) Clears the L2TP control channel authentication attribute-value (AV) pair counters.
id *local-id*	(Optional) Clears the per-tunnel control message counters for the L2TP tunnel with the specified local ID. The range is 1 to 4294967295.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(11)T	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

Use the **clear l2tp counters tunnel authentication** command to globally clear only the authentication counters.

Examples

The following example shows how to clear all L2TP tunnel counters:

```
Router# clear l2tp counters tunnel
```

The following example shows how to clear all L2TP tunnel authentication counters:

```
Router# clear l2tp counters tunnel authentication
```

Related Commands

Command	Description
show l2tp counters	Displays information about L2TP counters and tunnel statistics.
show l2tp session	Displays information about L2TP sessions.
show l2tp tunnel	Displays details about L2TP tunnels.

clear vpdn counters

To clear the counters of a specified virtual private dial-up network (VPDN) session or tunnel or to clear all of the VPDN counters, as displayed by the **show vpdn** command, use the **clear vpdn counters** command in privileged EXEC mode.

clear vpdn counters [**session** {**interface** *interface-type interface-number* | **id** *tunnel-id session-id* | **username** *username*} | **tunnel** {**l2f** | **l2tp** | **pptp**} {**all** | **hostname** *hostname* | **ip** {**remote** | **local**} *ip-address* | **id** *tunnel-id*}]

Syntax Description

session	(Optional) Specifies that session counters will be cleared.
interface *interface-type interface-number*	Clears VPDN session counters for the interface specified by the *interface-type interface-number* arguments. Valid values for the *interface-type* argument are: • **serial** --Specifies that VPDN session counters will be cleared on a serial interface. • **HSSI** --Specifies that VPDN session counters will be cleared on a High-Speed Serial Interface (HSSI). • **BRI** --Specifies that VPDN session counters will be cleared on a BRI interface. • **SUBIF** --Specifies that VPDN session counters will be cleared on an ATM or Frame Relay subinterface. • **Virtual-Access** --Specifies that VPDN session counters will be cleared on a virtual access interface.
id *tunnel-id session-id*	Clears VPDN session counters by tunnel and session ID. The range for the arguments is 1 to 65535.
username *username*	Clears VPDN session counters for the username specified by the *username* argument.
tunnel {**l2f** | **l2tp** | **pptp**}	(Optional) Clears both session and tunnel counters for the tunnel type specified by the **l2f**, **l2tp**, or the **pptp** keyword.
all	Clears VPDN counters for all sessions and tunnels of the selected tunnel type.

hostname *hostname*	Clears VPDN counters for all sessions and tunnels of the selected tunnel type associated with the particular host specified by the *hostname* argument. For the **l2tp** and the **pptp** tunnel type options, the *hostname* argument has the following value: *remote-name* [*local-name*] For the **l2f** tunnel type option, the *hostname* argument has the following value: *nas-name gateway-name* The *nas-name* argument is the name of the network access server and the *gateway-name* argument is the name of the home gateway.
ip {**remote** | **local**} *ip-address*	Clears VPDN counters for all sessions and tunnels of the selected tunnel type associated with the remote or local IP address specified by the *ip-address* argument.
id *tunnel-id*	Clears VPDN counters for all sessions and tunnels of the selected tunnel type associated with the tunnel id specified with the *tunnel-id* argument. The range is 1 to 65,535.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.4(11)T	The **l2f** keyword was removed.

Usage Guidelines

Use this command to clear counters for VPDN sessions and tunnels. If no keywords are used when the **clear vpdn counters** command is entered, all VPDN session and tunnel counters are cleared. If the **session** keyword is used, the specified session counters are cleared. If the **tunnel** keyword is used, the specified session and tunnel counters are cleared. You cannot clear the VPDN tunnel counters without also clearing the VPDN session counters.

Examples

The following example shows output from the **show vpdn** command before and after the **clear vpdn counters** command is issued:

```
Router# show vpdn session packets interface virtual-access 8
L2TP Session Information Total tunnels 1 sessions 1
```

```
PPTP session removal calls 0
LocID RemID TunID Pkts-In Pkts-Out Bytes-In Bytes-Out
7     2     28240 10282   10287    431844   298235
Router# clear vpdn counters session interface virtual-access 8

Clear "show vpdn" counters on this session [confirm]
Router# show vpdn session packets interface virtual-access 8
L2TP Session Information Total tunnels 1 sessions 1
PPTP session removal calls 0
LocID RemID TunID Pkts-In Pkts-Out Bytes-In Bytes-Out
7     2     28240 0       0        0        0
%No active PPTP tunnels
%No active PPPoE tunnels
```

Related Commands

Command	Description
show vpdn	Displays information about active L2TP tunnels or sessions in a VPDN.

clear vpdn dead-cache

To clear and restart a nonresponding (dead-cache state) Layer 2 Tunneling Protocol (L2TP) network access server (LNS), use the **clear vpdn dead-cache** command in user or in privileged EXEC mode.

clear vpdn dead-cache {**group** *group-name* | **ip-address** *ip-address* | **all**}

Syntax Description

group *group-name*	Clears all entries in the dead-cache for the specified VPDN group.
ip-address *ip-address*	Clears a specified entry in the dead-cache specified by its IP address.
all	Clears all entries in the dead-cache for all VPDN groups.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.2(31)ZV	This command was introduced.

Usage Guidelines

Use the **clear vpdn dead-cache** command to clear one or more LNS entries in the dead-cache. Once an LNS clears from the dead-cache, the LNS is active and available for new VPDN tunnels. Enter the **clear vpdn dead-cache** command on the L2TP access concentrator (LAC) gateway.

The **clear vpdn dead-cache group** command clears all dead-cache entries in the specified VPDN group To create a VPDN group and to enter VPDN group configuration mode, use the **vpdn-group** command in global configuration mode.

The **clear vpdn dead-cache ip address** command clears the specified IP address from all VPDN groups associated with that IP address.

Use the **show vpdn dead-cache** command in global configuration mode on the LNS gateway to display a list of LNS entries in a dead-cache state, including the IP address of the LNS and how long, in seconds, the entry has been in a dead-cache state.

To display an SNMP or system message log (syslog) event when an LNS enters or exits a dead-cache state, you must configure the **vpdn logging dead-cache** command.

Examples

The following example shows how to clear a specified entry in the dead-cache:

```
Router> enable
Router# clear vpdn dead-cache ip-address 10.10.10.1
```

The following example shows how to clear all entries in the dead-cache for a particular VPDN group:

```
Router> enable
Router# clear vpdn dead-cache group example
```

The following example shows how to clear all entries in the dead-cache for all VPDN groups:

```
Router> enable
Router# clear vpdn dead-cache all
```

Related Commands

Command	Description
show vpdn dead-cache	Displays a list of LNS entries in a dead-cache state, including the IP address of the LNS and how long, in seconds, the entry has been in a dead-cache state.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.
vpdn logging dead-cache	Enables the logging of VPDN events.

clear vpdn history failure

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

clear vpdn history failure

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.3T	This command was introduced.

Examples

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

```
Router# clear vpdn history failure
```

Related Commands

Command	Description
show vpdn history-failure	Displays the content of the failure history table.

clear vpdn redirect

To clear the Layer 2 Tunnel Protocol (L2TP) redirect counters shown in the **show vpdn redirect** command output, use the **clear vpdn redirect** command in privileged EXEC mode.

clear vpdn redirect

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(8)B	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

Use the **clear vpdn redirect** command to clear the statistics regarding redirects and forwards displayed by using the **show vpdn redirect** command.

Examples

The following example clears the redirect counters:

```
Router# clear vpdn redirect
```

Related Commands

Command	Description
show vpdn redirect	Displays statistics for L2TP redirects and forwards.
vpdn redirect	Enables L2TP redirect functionality.
vpdn redirect attempts	Restricts the number of redirect attempts possible for an L2TP call on the NAS.

Command	Description
vpdn redirect identifier	Configures a VPDN redirect identifier to use for L2TP call redirection on a stack group tunnel server.
vpdn redirect source	Configures the public redirect IP address of an L2TP stack group tunnel server.

clear vpdn tunnel

To shut down a specified virtual private dial-up network (VPDN) tunnel and all sessions within the tunnel, use the **clear vpdn tunnel** command in privileged EXEC mode.

L2TP or PPTP Tunnels

clear vpdn tunnel {**pptp** | **l2tp**} {**all** | **hostname** *remote-name* [*local-name*] | **id** *local-id* | **ip** *local-ip-address* | **ip** *remote-ip-address*}

L2F Tunnels

clear vpdn tunnel l2f {**all** | **hostname** *nas-name hgw-name* | **id** *local-id* | **ip** *local-ip-address* | **ip** *remote-ip-address*}

Syntax Description

pptp	Clears the specified Point-to-Point Tunneling Protocol (PPTP) tunnel.
l2tp	Clears the specified Layer 2 Tunneling Protocol (L2TP) tunnel.
all	Clears all VPDN tunnels terminating on the device.
hostname *remote-name* [*local-name*]	Clears all L2TP or PPTP VPDN tunnels established between the devices with the specified local and remote hostnames.
id *local-id*	Clears the VPDN tunnel with the specified local ID.
ip *local-ip-address*	Clears all VPDN tunnels terminating on the device with the specified local IP address.
ip *remote-ip-address*	Clears all VPDN tunnels terminating on the device with the specified remote IP address.
l2f	Clears the specified Layer 2 Forwarding (L2F) tunnel.
hostname *nas-name hgw-name*	Clears all L2F VPDN tunnels established between the network access server (NAS) and home gateway with the specified hostnames.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.2	This command was introduced.
11.3(5)AA	The **l2tp** keyword was added.
12.0(1)T	The **l2f** keyword was added.
12.0(5)XE5	The **pptp** keyword was added.
12.1(5)T	The **pptp** keyword was updated for additional Cisco access servers or routers.
12.2(2)T	The following keywords and arguments were added: • **all** • **hostname** *remote-name local-name* • **hostname** *nas-name hgw-name* • **id** *local-id* • **ip** *local-ip-address* • **ip** *remote-ip-address*
12.4(11)T	The **l2f** keyword was removed.

Usage Guidelines

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.

You can shut down VPDN tunnels more gradually by issuing the **vpdn softshut** command, which prevents the establishment of new VPDN sessions in all VPDN tunnels that terminate on the device. Existing VPDN sessions are not affected.

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. VPDN event logging is enabled by issuing the **vpdn logging** command.

Examples

The following example clears all L2TP tunnels connecting to a remote peer named NAS1:

```
Router# clear vpdn tunnel l2tp hostname NAS1
```

The following example clears all PPTP tunnels connecting the devices with the hostnames NAS3 and tun1:

```
Router# clear vpdn tunnel pptp NAS3 hostname tun1
```

This example shows the syslog messages that are displayed at both ends of the tunnel when the **clear vpdn tunnel l2tp all** command is entered at the LAC:

```
Router-LAC# clear vpdn tunnel l2tp all
00:01:29: %VPDN-6-CLOSED: L2TP LAC LAC closed  user user@surf1.org; Result 3, Error 6,
Admin Action
00:01:29: %VPDN-6-CLOSED: L2TP LAC closed tunnel  ; Result 1, Error 6, Admin Action
Router-LAC#
```

```
Router-LNS#
00:01:28: %VPDN-6-CLOSED: L2TP LAC closed tunnel  ; Result 1, Error 6, Admin Action
00:01:28: %VPDN-6-CLOSED: L2TP LAC LAC closed Vi2.1 user user@surf1.org; Result 3, Error
6, Admin Action
Router-LNS#
```

This example shows the syslog messages that are displayed at both ends of the tunnel when the **clear vpdn tunnel l2tp all** command is entered at the LNS:

```
Router-LNS# clear vpdn tunnel l2tp all
00:02:15: %VPDN-6-CLOSED: L2TP LNS LNS closed Vi2.1 user user@surf1.org; Result 3, Error
6, Admin Action
00:02:15: %VPDN-6-CLOSED: L2TP LNS closed tunnel  ; Result 1, Error 6, Admin Action
Router-LNS#
Router-LAC#
00:02:16: %VPDN-6-CLOSED: L2TP LNS closed tunnel  ; Result 1, Error 6, Admin Action
00:02:16: %VPDN-6-CLOSED: L2TP LNS LNS closed  user user@surf1.org; Result 3, Error 6,
Admin Action
Router-LAC#
```

Related Commands

Command	Description
vpdn logging	Enables the logging of generic VPDN events.
vpdn softshut	Prevents new sessions from being established on a VPDN tunnel without disturbing existing sessions.

clear vtemplate redundancy counters

To clear the virtual template redundancy counters in redundant systems that support broadband remote access server (BRAS) High Availability (HA), that are operating in Stateful Switchover (SSO) mode, use the **clear vtemplate redundancy counters** command in privileged EXEC mode.

clear vtemplate redundancy counters

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(32)SR	This command was introduced.

Usage Guidelines

Use the **clear vtemplate redundancy counters** command on either the Active or Standby route processor (RP). This command clears all the counters that are displayed using the **show vtemplate redundancy** command.

Use the **show vtemplate redundancy** command to ensure the virtual templates information is successfully synchronizing from the Active to the Standby RP.

Examples

The following is sample output from the **show vtemplate redundancy** command on the Active RP:

```
Router# show vtemplate redundancy
Global state                                  : Active - Dynamic Sync
ISSU state                                  : Compatible
Vaccess dynamic sync send                                 : 0
Vaccess dynamic sync send failed                                    : 0
Vaccess bulk sync send                                 : 24
Vaccess bulk sync send failed                                     : 0
Vaccess sync rcvd on standby                                    : 24
Vaccess recreate error on standby                                        : 0
```

The following is sample output from the **show vtemplate redundancy** command on the Standby RP:

```
Router-stdby# show vtemplate redundancy
Global state                                  : Active - Collecting
ISSU state                                  : Compatible
Vaccess dynamic sync send                                 : 0
Vaccess dynamic sync send failed                                    : 0
Vaccess bulk sync send                                 : 0
Vaccess bulk sync send failed                                     : 0
Vaccess sync rcvd on standby                                    : 24
Vaccess recreate error on standby                                        : 0
```

On the Standby RP, the first four counters do not increment. The value for Vaccess sync rcvd on the Standby RP should match the sum of the Vaccess bulk sync send and Vaccess dynamic sync send on the

Active RP. Any synchronization errors between the Active and Standby RPs increment the “failed” or “error” counters.

The following is sample output from the **clear vtemplate redundancy counters** command:

```
Router# clear vtemplate redundancy counters
Global state                                    : Active - Collecting
ISSU state                                     : Compatible
Vaccess dynamic sync send                                 : 0
Vaccess dynamic sync send failed                                : 0
Vaccess bulk sync send                                   : 0
Vaccess bulk sync send failed                                 : 0
Vaccess sync rcvd on standby                                 : 0
Vaccess recreate error on standby                                 : 0
```

Related Commands

Command	Description
show vtemplate redundancy	Displays synchronization information between the Active and Standby RPs.

default (VPDN)

To remove or reset a virtual private dialup network (VPDN) group or a VPDN subgroup configuration to its default value, use the **default** command in VPDN group, VPDN subgroup, or VPDN template configuration mode.

default *command*

Syntax Description

command	The command to be removed or reset from the VPDN group or VPDN subgroup configuration. The table below lists some of the commands that can be issued with the **default** command.

Command Default

No default behavior or values.

Command Modes

VPDN group configuration (config-vpdn)

VPDN subgroup configuration

VPDN template configuration (config-vpdn-temp)

Command History

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

Usage Guidelines

Use the **default** command to remove or reset a specific command configuration in a VPDN group, VPDN subgroup, or VPDN template configuration. Issuing **default** *command* is the same as issuing the **no** form of the command specified with the *command* argument.

The table below lists some of the commands that can be removed or reset using the **default** command, and the configuration modes that the **default** command must be issued in. Some commands might not be available unless a particular configuration is present on the router.

For a complete list of the commands available for use with the **default** command, use the **default ?** command in the desired configuration mode.

Some commands have required keywords or arguments that must be included in the **default** command statement. You can issue **default** *command* **?** to determine what keywords and arguments are required. For complete command syntax, see the command documentation in the *Cisco IOS Dial Technologies Command Reference*.

Table 2 Command Options for the default (VPDN) Command

Command Name	Configuration Mode
accept-dialin	VPDN group configuration mode.
accept-dialout	VPDN group configuration mode.
authen before-forward	VPDN group configuration mode.
dialer	Accept-dialout VPDN subgroup configuration mode.
dnis	Request-dialin VPDN subgroup configuration mode.
domain	Request-dialin VPDN subgroup configuration mode.
force-local-chap	VPDN group configuration mode.
initiate-to	VPDN group configuration mode.
lcp renegotiation	VPDN group configuration mode.
local name	VPDN group configuration mode.
multilink	VPDN group configuration mode.
pool-member	Request-dialout VPDN subgroup configuration mode.
protocol	Any VPDN subgroup configuration mode.
multihop	Request-dialin VPDN subgroup configuration mode.
request-dialin	VPDN group configuration mode.
request-dialout	VPDN group configuration mode.
rotary-group	Request-dialout VPDN subgroup configuration mode.
session-limit	VPDN group configuration mode.
source-ip	VPDN group configuration mode.
terminate-from	VPDN group configuration mode.
virtual-template	Accept-dialin VPDN subgroup configuration mode.

Examples

The following example shows the running configuration of a tunnel server VPDN group configured to accept Layer 2 Forwarding (L2F) dial-in calls and to place Layer 2 Tunneling Protocol (L2TP) dial-out calls:

```
Router# show running-config
!
vpdn-group group1
 accept-dialin
  protocol l2f
  virtual-template 1
 request-dialout
  protocol l2tp
  pool-member 1
 terminate-from hostname myhost
 initiate-to ip 10.3.2.1
 local name router32
 l2f ignore-mid-sequence
 l2tp ip udp checksum
!
```

If you issue the **default virtual-template** command in accept-dialin VPDN subgroup configuration mode, the **virtual-template** command configuration is removed from the VPDN subgroup:

```
Router(config-vpdn-req-out)# default virtual-template
!
Router# show running-config
!
vpdn-group group1
 accept-dialin
  protocol l2f
 request-dialout
  protocol l2tp
  pool-member 1
 terminate-from hostname myhost
 initiate-to ip 10.3.2.1
 local name router32
 l2f ignore-mid-sequence
 l2tp ip udp checksum
!
```

If you issue the **default accept-dialin** command in VPDN group configuration mode, the accept-dialin VPDN subgroup configuration is removed from the VPDN group along with all configurations that require an accept-dialin VPDN subgroup:

```
Router(config-vpdn)# default accept-dialin
!
Router# show running-config
!
vpdn-group group1
 request dialout
  protocol l2tp
  pool-member 1
 local name router32
 initiate-to ip 10.3.2.1
 l2tp ip udp checksum
```

The following example enters VPDN template configuration mode and uses the command line help system to find the commands available to use with the **default** command:

```
Router(config)# vpdn-template 1
Router(config-vpdn-templ)# default ?
  description  Description for this VPDN group
  group        Items grouped for all attached vpdn-groups
  ip           IP settings for tunnel
  l2f          L2F specific commands
  l2tp         L2TP specific commands
  local        Local information
  pptp         PPTP specific commands
```

```
  redirect     Call redirection options
  relay        Relay options configuration
  vpn          VPN ID/VRF name
```

The following example uses the command line help system to show that a value must be entered for the *number* argument when the **default session-limit** command is issued in VPDN group configuration mode:

```
Router(config-vpdn)# default session-limit ?
  <0-32767>  Max number of sessions
```

Related Commands

Command	Description
accept-dialin	Creates an accept dial-in VPDN subgroup that configures a tunnel server to accept requests from a NAS to tunnel dial-in calls, and enters accept-dialin VPDN subgroup configuration mode.
accept-dialout	Creates an accept dial-out VPDN subgroup that configures a NAS to accept requests from a tunnel server to tunnel L2TP dial-out calls, and enters accept-dialout VPDN subgroup configuration mode.
request-dialin	Creates a request dial-in VPDN subgroup that configures a NAS to request the establishment of a dial-in tunnel to a tunnel server, and enters request-dialin VPDN subgroup configuration mode.
request-dialout	Creates a request dial-out VPDN subgroup that configures a tunnel server to request the establishment of dial-out L2TP tunnels to a NAS, and enters request-dialout VPDN subgroup configuration mode.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.
vpdn-template	Enters VPDN template configuration mode, where a template for VPDN groups can be configured.

description (VPDN group)

To add a description to a virtual private dialup network (VPDN) group, use the **description** command in VPDN group or VPDN template configuration mode. To remove the description, use the **no** form of this command.

description *string*

no description

Syntax Description

string	Comment or a description about the VPDN group.

Command Default

No description is associated with the VPDN group.

Command Modes

VPDN group configuration (config-vpdn)

VPDN template configuration (config-vpdn-temp)

Command History

Release	Modification
12.2	This command was introduced.

Examples

The following example shows how to enter a description for a VPDN group:

```
vpdn-group 333
 description This is a VPDN group at location 333
 request-dialin
  protocol l2tp
  domain cisco2.com
  exit
 initiate-to ip 10.0.0.63
 local name cisco.com
```

Related Commands

Command	Description
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.
vpdn-template	Creates a VPDN template and enters VPDN template configuration mode.

dialer vpdn

To enable a dialer profile or dial-on-demand routing (DDR) dialer to use Layer 2 Tunneling Protocol (L2TP) dialout, use the **dialer vpdn** command in interface configuration mode. To disable L2TP dialout on a dialer profile or DDR dialer, use the **no** form of this command.

dialer vpdn

no dialer vpdn

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

The **dialer vpdn** command must be configured on the L2TP network servers (LNSs) dialer interface to enable L2TP dialout. This command enables the dialer to place a VPDN call.

Examples

The following example shows how to configure the dialer interface and VPDN group on an LNS for L2TP dialout:

```
interface Dialer2
 ip address 172.16.2.3 255.255.255.128
 encapsulation ppp
 dialer remote-name myname
 dialer string 5550134
 dialer vpdn
 dialer pool 1
 dialer-group 1
 ppp authentication chap
vpdn-group 1
 request-dialout
  protocol l2tp
  pool-member 1
 initiate-to ip 172.21.9.4
```

Related Commands

Command	Description
dialer aaa	Allows a dialer to access the AAA server for dialing information.
request-dialout	Enables an LNS to request VPDN dial-out calls by using L2TP.

dnis (VPDN)

To specify the Dialed Number Identification Service (DNIS) group name or DNIS number of users that are to be forwarded to a tunnel server using a virtual private dialup network (VPDN), use the **dnis** command in request dial-in VPDN subgroup configuration mode. To remove a DNIS group or number from a VPDN group, use the **no** form of this command.

dnis {*dnis-group-name* | *dnis-number*}

no dnis {*dnis-group-name* | *dnis-number*}

Syntax Description

dnis-group-name	DNIS group name used when resource pool management (RPM) is enabled and the VPDN group is configured under the incoming customer profile.
dnis-number	DNIS group number used when RPM is disabled, or when a call is associated with a customer profile without any VPDN group configured for the customer profile.

Command Default

Disabled

Command Modes

Request dial-in VPDN subgroup configuration (config-vpdn-req-in)

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Usage Guidelines

You must specify a tunneling protocol by using the **protocol** command in request dial-in VPDN subgroup configuration mode before issuing the **dnis** command. Removing or changing the **protocol** command configuration removes any existing **dnis** command configuration from the request dial-in VPDN subgroup.

You can configure a VPDN group to tunnel multiple DNIS group names and DNIS numbers by issuing multiple instances of the **dnis** command.

VPDN groups can also be configured to tunnel users based on domain name by using the **domain** command.

Examples

The following example configures a VPDN group to tunnel calls from multiple DNIS numbers and from the domain cisco.com to the tunnel server at 10.1.1.1 using the Layer 2 Forwarding (L2F) protocol:

Note Effective with Cisco Release 12.4(11)T, the L2F protocol is not supported in Cisco IOS software.

```
Router(config)# vpdn-group users
Router(config-vpdn)# request dialin
Router(config-vpdn-req-in)# protocol l2f
Router(config-vpdn-req-in)# dnis 1234
Router(config-vpdn-req-in)# dnis 5678
Router(config-vpdn-req-in)# domain cisco.com
!
Router(config-vpdn)# initiate-to 10.1.1.1
```

Related Commands

Command	Description
dialer dnis group	Creates a DNIS group.
domain	Specifies the domain name of users that are to be forwarded to a tunnel server using VPDN.
dnis group	Includes a group of DNIS numbers in a customer profile.
protocol (VPDN)	Specifies the tunneling protocol that the VPDN subgroup will use.
request-dialin	Creates a request dial-in VPDN subgroup that configures a NAS to request the establishment of a dial-in tunnel to a tunnel server, and enters request dial-in VPDN subgroup configuration mode.

domain

To specify the domain name of users that are to be forwarded to a tunnel server using a virtual private dialup network (VPDN), use the **domain** command in request dial-in VPDN subgroup configuration mode. To remove a domain from a VPDN group or subgroup, use the **no** form of this command.

domain *domain-name*

no domain [*domain-name*]

Syntax Description

domain-name	Case-sensitive name of the domain that will be tunneled.

Command Default

Disabled

Command Modes

Request dial-in VPDN subgroup configuration (config-vpdn-req-in)

Command History

Release	Modification
12.0(4)XI	This command was introduced.
12.0(5)T	This command was integrated into Cisco IOS Release 12.0(5)T.

Usage Guidelines

You must specify a tunneling protocol by using the **protocol** command in request dial-in VPDN subgroup configuration mode before issuing the **domain** command. Removing or changing the **protocol** command configuration removes any existing **domain** command configuration from the request dial-in VPDN subgroup.

You can configure a request dial-in VPDN subgroup to tunnel calls from multiple domain names by issuing multiple instances of the **domain** command.

VPDN groups can also be configured to tunnel users based on Dialed Number Identification Service (DNIS) group names or DNIS numbers by using the **dnis** command.

Examples

The following example configures VPDN group 1 to request a dial-in Layer 2 Tunnel Protocol (L2TP) tunnel to IP address 10.99.67.76 when it receives a PPP call from a username with the domain name cisco1.com, the domain name cisco2.com, or the DNIS number 4321:

```
Router(config)# vpdn-group 1
```

```
Router(config-vpdn)# request-dialin
Router(config-vpdn-req-in)# protocol l2tp
Router(config-vpdn-req-in)# domain cisco1.com
Router(config-vpdn-req-in)# domain cisco2.com
Router(config-vpdn-req-in)# dnis 4321
!
Router(config-vpdn)# initiate-to ip 10.99.67.76
```

Related Commands

Command	Description
dnis	Specifies the DNIS group name or DNIS number of users that are to be forwarded to a tunnel server using VPDN.
protocol (VPDN)	Specifies the tunneling protocol that the VPDN subgroup will use.
request-dialin	Creates a request dial-in VPDN subgroup that configures a NAS to request the establishment of a dial-in tunnel to a tunnel server, and enters request dial-in VPDN subgroup configuration mode.

dsl-line-info-forwarding

To enable processing of the attribute-value (AV) pairs containing Digital Subscriber Line (DSL) information in a PPPoE Active Discovery Request (PADR) packet, and send the AV pair from the Layer 2 Tunneling Protocol (L2TP) access concentrator (LAC) to the L2TP network server (LNS) where a matching Vendor Specific Attribute (VSA) is sent to an authentication, authorization, and accounting (AAA) server for authentication, authorization, and accounting, use the **dsl-line-info-forwarding** command in VPDN group or VPDN template configuration mode. To disable the command function, use the **no** form of this command.

dsl-line-info-forwarding

no dsl-line-info-forwarding

Syntax Description

This command has no arguments or keywords.

Command Default

The command function is disabled.

Command Modes

VPDN group configuration (config-vpdn)

VPDN template configuration (config-vpdn-temp)

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

Configure the **dsl-line-info-forwarding** command on the LAC.

Examples

The following example shows the configuration on the LAC:

```
LAC(config)# vpdn-group example
LAC(config)# dsl-line-info-forwarding
```

The following example shows the ICRQ message containing the circuit-id, shown in bold, when you configure the **dsl-line-info-forwarding** command on the LAC:

```
03:11:49:L2TPtnl 61454:42513: | ICRQ, flg TLS, ver 2, len 90
03:11:49:L2TPtnl 61454:42513: tnl 42513, ns 2, nr 1
03:11:49:L2TPtnl 61454:42513: IETF v2:
03:11:49:L2TPtnl 61454:42513: Assigned Call ID 24
03:11:49:L2TPtnl 61454:42513: Serial Number 12345
03:11:49:L2TPtnl 61454:42513: Bearer Type none (0)
03:11:49:L2TPtnl 61454:42513: Cisco v2:
```

```
03:11:49:L2TPtnl 61454:42513: Client NAS Port [9]
03:11:49:L2TPtnl 61454:42513:
"<0F><10><09><02><02><Qg<00><00>"
03:11:49:L2TPtnl 61454:42513: ADSL Forum v2:
03:11:49:L2TPtnl 61454:42513: Circuit ID [21]
03:11:49:L2TPtnl 61454:42513: "Ethernet1/1:PPOE-TAG"
```

The following example shows the ICRQ message containing no circuit-id, when you configure the **no dsl-line-info-forwarding** command on the LAC:

```
03:11:49:L2TPtnl 61454:42513: | ICRQ, flg TLS, ver 2, len 90
03:11:49:L2TPtnl 61454:42513: tnl 42513, ns 2, nr 1
03:11:49:L2TPtnl 61454:42513: IETF v2:
03:11:49:L2TPtnl 61454:42513: Assigned Call ID 24
03:11:49:L2TPtnl 61454:42513: Serial Number 12345
03:11:49:L2TPtnl 61454:42513: Bearer Type none (0)
03:11:49:L2TPtnl 61454:42513: Cisco v2:
03:11:49:L2TPtnl 61454:42513: Client NAS Port [9]
03:11:49:L2TPtnl 61454:42513:
"<0F><10><09><02><02><Qg<00><00>"
```

Related Commands

Command	Description
debug vpdn	Displays information associated with the RADIUS server.
radius server attribute 87 circuit-id	Overrides the nas-port-id attribute with circuit-id in RADIUS AAA messages.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.

encryption mppe

To enable Microsoft Point-to-Point Encryption (MPPE) on an Industry-Standard Architecture (ISA) card, use the **encryption mppe** command in controller configuration mode. To disable MPPE, use the **no** form of this command.

encryption mppe

no encryption mppe

Syntax Description

This command has no arguments or keywords.

Command Default

IPSec is the default encryption type.

Command Modes

Controller configuration (config-controller)

Command History

Release	Modification
12.0(5)XE5	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Usage Guidelines

Using the ISA card offloads MPPE from the Route Processor and improves performance in large-scale environments.

The router must be rebooted for the change to the **encryption mppe** command configuration to take effect.

Examples

The following example enables MPPE encryption on the ISA card in slot 5, port 0:

```
Router(config)# controller isa 5/0
Router(config-controller)# encryption mppe
```

Related Commands

Command	Description
debug ppp mppe	Displays debug messages for MPPE events.
encryption mppe	Enables MPPE encryption on the virtual template.

Command	Description
show ppp mppe	Displays MPPE information for an interface.

force-local-chap

To force the Layer 2 Tunneling Protocol (L2TP) network server (LNS) to reauthenticate the client, use the **force-local-chap** command in VPDN group configuration mode. To disable reauthentication, use the **no** form of this command.

force-local-chap

no force-local-chap

Syntax Description

This command has no arguments or keywords.

Command Default

Proxy authentication. The Challenge Handshake Authentication Protocol (CHAP) response to the L2TP access concentrator (LAC) authentication challenge is passed to the LNS.

Command Modes

VPDN group configuration (config-vpdn)

Command History

Release	Modification
11.3(5)AA	This command was introduced.
12.0(1)T	This command was integrated into Cisco IOS Release 12.0(1)T.
12.0(5)T	This command was modified to be available only if the accept-dialin VPDN group configuration mode is enabled.

Usage Guidelines

You must enable the **accept-dialin** command on the VPDN group before you can use the **force-local-chap** command. Removing the **accept-dialin** command removes the **force-local-chap** command from the VPDN group.

This command is used only if CHAP authentication is enabled for PPP (using the **ppp authentication chap** command). This command forces the LNS to reauthenticate the client in addition to the proxy authentication that occurs at the LAC. If the **force-local-chap** command is used, then the authentication challenge occurs twice. The first challenge comes from the LAC, and the second challenge comes from the LNS. Some PPP clients might experience problems with double authentication. If this problem occurs, authentication challenge failures might be seen if the **debug ppp authentication** command is enabled.

Examples

The following example enables CHAP authentication at the LNS:

```
vpdn-group 1
 accept dialin
  protocol l2tp
  virtual-template 1
terminate-from hostname router32
 force-local-chap
```

Related Commands

Command	Description
accept-dialin	Configures an LNS to accept tunneled PPP connections from a LAC and create an accept dial-in VPDN subgroup.
lcp renegotiation	Allows the LNS to renegotiate the LCP on dial-in calls, using L2TP or L2F.

group session-limit

To limit the number of simultaneous virtual private dialup network (VPDN) sessions allowed across all VPDN groups associated with a particular VPDN template, use the **group session-limit** command in VPDN template configuration mode. To remove a configured session limit restriction, use the **no** form of this command.

group session-limit *number*

no group session-limit

Syntax Description

number	Maximum number of concurrent sessions allowed across all VPDN groups associated with a particular VPDN template. The range is 1 to 32767.

Command Default

No session limit exists for the VPDN template.

Command Modes

VPDN template configuration (config-vpdn-temp)

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.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

Use the **group session-limit** command to specify the maximum number of simultaneous sessions allowed across all VPDN groups associated with a VPDN template.

If you configure a session limit that is less than the number of current active sessions, existing sessions are not terminated. However, new sessions are not established until the number of existing sessions falls below the configured session limit.

VPDN session limits can be configured globally by using the **vpdn session-limit** command, at the level of a VPDN group by using the **session-limit** (VPDN) command, or for all VPDN groups associated with a particular VPDN template by using the **group session-limit** command.

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 cannot 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 cannot exceed the configured VPDN template session limit.
- Session limits configured for a VPDN group are enforced for that VPDN group.

Examples

The following example associates two VPDN groups with the VPDN template named cisco, and configures a session limit of 100 for all VPDN groups associated with the template:

```
vpdn-group group1
 source vpdn-template cisco
!
vpdn-group group2
 source vpdn-template cisco
!
vpdn-template cisco
 group session-limit 100
```

Related Commands

Command	Description
session-limit (VPDN)	Limits the number of simultaneous VPDN sessions allowed for a specified VPDN group.
show vpdn session	Displays session information about active Layer 2 sessions for a VPDN.
source vpdn-template	Associates a VPDN group with a VPDN template.
vpdn session-limit	Limits the number of simultaneous VPDN sessions allowed on a router.
vpdn-template	Creates a VPDN template and enters VPDN template configuration mode.

initiate-to

To specify an IP address that will be used for Layer 2 tunneling, use the **initiate-to** command in VPDN group configuration mode. To remove an IP address from the virtual private dialup network (VPDN) group, use the **no** form of this command.

initiate-to ip *ip-address* [**limit** *limit-number*] [**priority** *priority-number*]

no initiate-to [**ip** *ip-address*]

Syntax Description

ip *ip-address*	Specifies the IP address of the router that will be tunneled to.
limit *limit-number*	(Optional) Specifies a limit to the number of connections that can be made to this IP address in the range of 0 to 32767.
priority *priority-number*	(Optional) Specifies a priority for this IP address in the range of 1 to 32767. 1 is the highest priority.

Command Default

No IP address is specified.

Command Modes

VPDN group configuration (config-vpdn)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(15)T	This command was enhanced with the capability to configure multiple Layer 2 Tunneling Protocol (L2TP) network access servers (NASs) on an L2TP tunnel server within the same VPDN group.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Before you can use this command, you must enable one of the two request VPDN subgroups by using either the **request-dialin** or the **request-dialout** command.

A NAS configured to request dial-in can be configured with multiple **initiate-to** commands to enable tunneling to more than one IP address.

A tunnel server configured to request dial-out can be configured with multiple **initiate-to** commands to enable tunneling to more than one IP address.

Examples

The following example configures a VPDN group for L2TP dial-out. This group can tunnel a maximum of five simultaneous users and has the second highest priority for requesting dial-out calls.

```
vpdn-group 1
 request-dialout
 protocol l2tp
 pool-member 1
!
 initiate-to ip 10.3.2.1 limit 5 priority
```

The following example configures VPDN group 1 to request L2TP tunnels to the peers (NASs) at IP addresses 10.0.58.201 and 10.0.58.205. The two NASs configured by the **initiate-to** commands have differing priority values to provide failover redundancy.

```
vpdn-group 1
 accept-dialin
 protocol l2tp
 virtual-template 1
!
 request-dialout
 protocol l2tp
 pool-member 1
!
 initiate-to ip 10.0.58.201  priority 1
 initiate-to ip 10.0.58.205  priority 100
 source-ip 10.0.58.211
```

In the previous example, you would configure load balancing among the NASs by setting the **priority** values in the **initiate-to** commands to the same values.

The following partial example shows how to set parameters to control how many times a tunnel server retries connecting to a NAS, and the amount of time after which the NAS declares itself down or busy so that the tunnel server tries connecting to the next NAS. (Note that the **l2tp tunnel** commands are optional and should be used only if it becomes necessary to change the default settings for these commands.)

```
!
vpdn enable
vpdn search-order domain
!
vpdn-group 1
.
.
.
 request-dialout
 protocol l2tp
 pool-member 1
!
 initiate-to ip 10.0.58.201 priority 1
 initiate-to ip 10.0.58.207 priority 50
 initiate-to ip 10.0.58.205 priority 100
 l2tp tunnel retransmit initial retries 5
 l2tp tunnel retransmit initial timeout min 4
 l2tp tunnel busy timeout 420
.
.
.
```

Related Commands

Command	Description
l2tp tunnel busy timeout	Configures the amount of time that the router waits before attempting to recontact a router that was previously busy.
l2tp tunnel retransmit initial retries	Sets the number of times that the router attempts to send out the initial control packet for tunnel establishment before considering a router busy.
l2tp tunnel retransmit initial timeout	Sets the minimum or maximum amount of time that the router waits before resending an initial packet out to establish a tunnel.
request-dialin	Creates a request dial-in VPDN subgroup that configures a NAS to request the establishment of a dial-in tunnel to a tunnel server, and enters request dial-in VPDN subgroup configuration mode.
request-dialout	Creates a request dial-out VPDN subgroup that configures a tunnel server to request the establishment of dial-out L2TP tunnels to a NAS, and enters request dial-out VPDN subgroup configuration mode.
source-ip	Specifies an alternate IP address for a VPDN tunnel that is different from the physical IP address used to open the tunnel.

interface virtual-template

To create a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces, use the **interface virtual-template** command in global configuration mode. To remove a virtual template interface, use the **no** form of this command.

interface virtual-template *number* [**type** *virtual-template-type*]

no interface virtual-template *number*

Syntax Description

number	Number used to identify the virtual template interface. Up to 200 virtual template interfaces can be configured. On the Cisco 10000 series router, up to 4095 virtual template interfaces can be configured.
type *virtual-template-type*	(Optional) Specifies the type of virtual template.

Command Default

No virtual template interface is defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.2F	This command was introduced.
12.2(4)T	This command was enhanced to increase the maximum number of virtual template interfaces from 25 to 200.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Release	Modification
12.2(33)SB	This command default configuration was modified for SNMP and implemented on the Cisco 10000 series router for the PRE3 and PRE4.
Cisco IOS XE Release 2.5	This command was implemented on Cisco ASR 1000 series routers.

Usage Guidelines

A virtual template interface is used to provide the configuration for dynamically created virtual access interfaces. It is created by users and can be saved in NVRAM.

After the virtual template interface is created, it can be configured in the same way as a serial interface.

Virtual template interfaces can be created and applied by various applications such as virtual profiles, virtual private dialup networks (VPDNs), PPP over ATM, protocol translation, and Multichassis Multilink PPP (MMP).

You can configure up to 4095 total virtual template interfaces on the Cisco 10000 series router.

To ensure proper scaling and to minimize CPU utilization, we recommend these virtual template interface settings:

- A keepalive timer of 30 seconds or greater by using the **keepalive** command. The default is 10 seconds.
- Do not enable the Cisco Discovery Protocol (CDP). CDP is disabled by default. Use the **no cdp enable** command to disable CDP, if necessary.
- Disable link-status event messaging by using the **no logging event link-status** command.
- To prevent the virtual-access subinterfaces from being registered with the SNMP functionality of the router and using memory, do not use the router's SNMP management tools to monitor PPP sessions. Use the **no virtual-template snmp** command to disable the SNMP management tools.

When a virtual template interface is applied dynamically to an incoming user session, a virtual access interface (VAI) is created.

If you configure a virtual template interface with interface-specific commands, the Cisco 10000 series router does not achieve the highest possible scaling. To verify that the router does not have interface-specific commands within the virtual template interface configuration, use the **test virtual-template** *number* **subinterface** command.

In Cisco IOS Release 12.2(33)SB, the default configuration for the **virtual-template snmp** command was changed to **no virtual-template snmp**. This prevents large numbers of entries into the MIB ifTable, thereby avoiding CPU Hog messages as SNMP uses the interfaces MIB and other related MIBs. If you configure the **no virtual-template snmp** command, the router no longer accepts the **snmp trap link-status** command under a virtual-template interface. Instead, the router displays a configuration error message such as the following:

```
Router(config)# interface virtual-template 1
Router(config-if)# snmp trap link-status
%Unable set link-status enable/disable for interface
```

If your configuration already has the **snmp trap link-status** command configured under a virtual-template interface and you upgrade to Cisco IOS Release 12.2(33)SB, the configuration error occurs when the router reloads even though the virtual template interface is already registered in the interfaces MIB.

Examples

The following example creates a virtual template interface called Virtual-Template1:

```
Router(config)# interface Virtual-Template1
Router(config-if)# ip unnumbered Loopback1
Router(config-if)# keepalive 60
Router(config-if)# no peer default ip address
Router(config-if)# ppp authentication pap
Router(config-if)# ppp authorization vpn1
Router(config-if)# ppp accounting vpn1
Router(config-if)# no logging event link-status
Router(config-if)# no virtual-template snmp
```

The following example creates and configures virtual template interface 1:

```
interface virtual-template 1 type ethernet
 ip unnumbered ethernet 0
 ppp multilink
 ppp authentication chap
```

The following example shows how to configure a virtual template for an IPsec virtual tunnel interface.

```
interface virtual-template1 type tunnel
 ip unnumbered Loopback1
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile virtualtunnelinterface
```

Related Commands

Command	Description
cdp enable	Enables CDP on an interface.
clear interface virtual-access	Tears down the live sessions and frees the memory for other client uses.
keepalive	Enables keepalive packets and specifies the number of times that the software tries to send keepalive packets without a response before bringing down the interface.
show interface virtual-access	Displays the configuration of the active VAI that was created using a virtual template interface.
tunnel protection	Associates a tunnel interface with an IPsec profile.
virtual interface	Sets the zone name for the connected AppleTalk network.
virtual-profile	Enables virtual profiles.
virtual template	Specifies the destination for a tunnel interface.

ip mtu adjust

To enable automatic adjustment of the IP maximum transmission unit (MTU) on a virtual access interface, use the **ip mtu adjust** command in VPDN group or VPDN template configuration mode. To disable automatic adjustment of the IP MTU, use the **no** form of this command.

ip mtu adjust

no ip mtu adjust

Syntax Description

This command has no arguments or keywords.

Command Default

For Cisco IOS Release 12.2(3) and 12.2(4)T: Automatic adjustment of the IP MTU is enabled.

For Cisco IOS Release 12.2(6) and 12.2(8)T and later releases: Automatic adjustment of the IP MTU is disabled.

Command Modes

VPDN group configuration (config-vpdn)

VPDN template configuration (config-vpdn-temp)

Command History

Release	Modification
12.2(3)	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(6)	The default setting for this command was changed from enabled to disabled.
12.2(8)T	The default setting for this command was changed from enabled to disabled.

Usage Guidelines

Enabling the **ip mtu adjust** command allows the router to automatically adjust the IP MTU on the virtual access interface associated with the specified virtual private dialup network (VPDN) group. The IP MTU is automatically adjusted to compensate for the size of the Layer 2 header and the MTU of the egress interface.

The IP MTU is adjusted automatically only if there is no IP MTU manually configured on the virtual template interface from which the virtual access interface is cloned. To manually configure an IP MTU on the virtual template interface, use the **ip mtu** command in interface configuration mode.

Examples

The following example enables automatic adjustment of the IP MTU for sessions associated with the VPDN group named cisco1:

```
vpdn-group cisco1
 ip mtu adjust
```

Related Commands

Command	Description
ip mtu	Sets the MTU size of IP packets sent on an interface.
ip pmtu	Allows VPDN tunnels to participate in path MTU discovery.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.
vpdn-template	Creates a VPDN template and enters VPDN template configuration mode.

ip pmtu

To enable the discovery of the path maximum transmission unit (MTU) for Layer 2 traffic, use the **ip pmtu** command in VPDN group, VPDN template, or pseudowire class configuration mode. To disable path MTU discovery, use the **no** form of this command.

ip pmtu
no ip pmtu

Syntax Description

This command has no arguments or keywords.

Command Default

Path MTU discovery is disabled.

Command Modes

VPDN group configuration (config-vpdn)
VPDN template configuration (config-vpdn-temp)
Pseudowire class configuration (config-pw)

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(11)T	This command was implemented on the Cisco 1760, Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S and support was added for using this command in pseudowire class configuration mode.
12.3(2)T	Support was added for using this command in pseudowire class configuration mode.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
Cisco IOS XE Release 2.6.2	This command was integrated into Cisco IOS XE Release 2.6.2.

Usage Guidelines

When the **ip pmtu** command is enabled, the Don't Fragment (DF) bit is copied from the inner IP header to the Layer 2 encapsulation header.

Enabling the **ip pmtu** command triggers Internet Control Message Protocol (ICMP) unreachable messages, which indicate fragmentation errors occurred in the IP backbone network carrying the tunneled traffic. If an IP packet is larger than the MTU of any interface, it must pass through, the DF bit is set, the packet is dropped, and an ICMP unreachable message is returned. The ICMP unreachable message indicates the MTU of the interface was unable to forward the packet without fragmentation. This information allows the source host to reduce the size of the packet before retransmission, allowing it to fit through that interface.

Note When path MTU discovery (PMTUD) is enabled, VPDN deployments are vulnerable to Denial of Service (DoS) attacks that use crafted Internet Control Message Protocol (ICMP) "fragmentation needed and Don't Fragment (DF) bit set" (code 4) messages, also known as PMTUD attacks. Crafted code 4 ICMP messages can be used to set the path MTU to an impractically low value. This will cause higher layer protocols to time out because of a very low throughput even though the connection is still in the established state. This type of attack is classified as a throughput-reduction attack. When PMTUD is enabled, we recommend that you use the **vpdn pmtu** command to configure a range of acceptable values for the path MTU to block PMTUD attacks.

Enabling PMTUD will decrease switching performance.

When issued in VPDN group configuration mode, the **ip pmtu** command enables any tunnel associated with the specified virtual private dialup network (VPDN) group to participate in path MTU discovery.

When issued in VPDN template configuration mode, the **ip pmtu** command enables any tunnel associated with the specified VPDN template to participate in path MTU discovery.

When issued in pseudowire class configuration mode, the **ip pmtu** command enables any Layer 2 Tunneling Protocol Version 3 (L2TPv3) session derived from the specified pseudowire class configuration to participate in path MTU discovery.

Examples

The following example configures a VPDN group named dial-in on an L2TP tunnel server and uses the **ip pmtu** command to specify that tunnels associated with this VPDN group will participate in path MTU discovery. The **vpdn pmtu** command configures the device to accept only path MTU values ranging from 576 to 1460 bytes. The device ignores code 4 ICMP messages that specify a path MTU outside of this range.

```
Router(config)# vpdn-group dial-in
Router(config-vpdn)# request-dialin
Router(config-vpdn-acc-in)# protocol l2tp
Router(config-vpdn-acc-in)# virtual-template 1
!
Router(config-vpdn)# l2tp security crypto-profile l2tp
Router(config-vpdn)# no l2tp tunnel authentication
Router(config-vpdn)# lcp renegotiation on-mismatch
Router(config-vpdn)# ip pmtu
!
Router(config)# vpdn pmtu maximum 1460
Router(config)# vpdn pmtu minimum 576
```

The following example shows how to enable the discovery of the path MTU for pseudowires that are created from the pseudowire class named ether-pw. The **vpdn pmtu** command configures the device to accept only path MTU values ranging from 576 to 1460 bytes. The device ignores code 4 ICMP messages that specify a path MTU outside of this range.

```
Router(config)# pseudowire-class ether-pw
```

```
Router(config-pw)# ip pmtu
!
Router(config)# vpdn pmtu maximum 1460
Router(config)# vpdn pmtu minimum 576
```

Related Commands

Command	Description
ip dfbit set	Enables the DF bit in the outer L2TPv3 tunnel header.
ip mtu	Sets the MTU size of IP packets sent on an interface.
ip mtu adjust	Enables automatic adjustment of the IP MTU on a virtual access interface.
pseudowire-class	Specifies the name of an L2TP pseudowire class and enters pseudowire class configuration mode.
vpdn pmtu	Manually configures a range of allowed path MTU sizes for an L2TP VPDN.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.
vpdn-template	Creates a VPDN template and enters VPDN template configuration mode.

ip precedence (VPDN)

To set the precedence value in the virtual private dialup network (VPDN) Layer 2 encapsulation header, use the **ip precedence** command in VPDN group or VPDN template configuration mode. To remove a precedence value setting, use the **no** form of this command.

ip precedence {*number* | *name*}

no ip precedence {*number* | *name*}

Syntax Description

number | *name*	A number or name that defines the setting for the precedence bits in the IP header. The values for the arguments are listed in the table below, from least to most important.

Command Default

The IP precedence value of the Layer 2 encapsulation header is set to zero.

Command Modes

VPDN group configuration (config-vpdn)

VPDN template configuration (config-vpdn-temp)

Command History

Release	Modification
12.1(1.1)	This command was introduced.
12.1(1.1)T	This command was integrated into Cisco IOS Release 12.1(1.1)T.

Usage Guidelines

The table below lists the values for the arguments for precedence values in the IP header. They are listed from least to most important.

Table 3 Number and Name Values for IP Precedence

Number	Name
0	**routine**
1	**priority**
2	**immediate**

Number	Name
3	**flash**
4	**flash-override**
5	**critical**
6	**internet**
7	**network**

You can set the precedence using either a number or the corresponding name. Once the IP Precedence bits are set, other quality of service (QoS) services such as weighted fair queueing (WFQ) and Weighted Random Early Detection (WRED) then operate on the bit settings.

For more information about QoS services, see the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Examples

The following example sets the IP precedence to 5 (critical) for packets that traverse the VPDN tunnel associated with VPDN group 1:

```
vpdn-group 1
 ip precedence 5
```

Related Commands

Command	Description
ip tos	Sets the ToS bits in the VPDN Layer 2 encapsulation header.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.
vpdn-template	Creates a VPDN template and enters VPDN template configuration mode.

ip tos (VPDN)

To set the type of service (ToS) bits in the virtual private dialup network (VPDN) Layer 2 encapsulation header, use the **ip tos** command in VPDN group or VPDN template configuration mode. To restore the default setting, use the **no** form of this command.

ip tos {*tos-bit-value* | **max-reliability** | **max-throughput** | **min-delay** | **min-monetary-cost** | **normal** | **reflect**}

no set ip tos {*tos-bit-value* | **max-reliability** | **max-throughput** | **min-delay** | **min-monetary-cost** | **normal** | **reflect**}

Syntax Description

tos-bit-value	A number from 0 to 15 that sets the ToS bits in the IP header. See the table below for more information.
max-reliability	Sets the maximum reliability ToS bits to 2.
max-throughput	Sets the maximum throughput ToS bits to 4.
min-delay	Sets the minimum delay ToS bits to 8.
min-monetary-cost	Sets the minimum monetary cost ToS bits to 1.
normal	Sets the normal ToS bits to 0. This is the default setting.
reflect	Copies the ToS value from the inner IP packet to the Layer 2 encapsulation header.

Command Default

The ToS bits are set to 0, which is equivalent to the **normal** keyword.

Command Modes

VPDN group configuration (config-vpdn)

VPDN template configuration (config-vpdn-temp)

Command History

Release	Modification
12.0(5)T	This command was introduced as **l2tp ip tos reflect**.
12.1(1.1)	The **l2tp ip tos reflect** command was replaced by the **ip tos** command, configuration options were added, and support was added for other protocols.

Release	Modification
12.1(1.1)T	This command was integrated into Cisco IOS Release 12.1(1.1)T

Usage Guidelines

The **ip tos** command allows you to set four bits in the ToS portion of the Layer 2 encapsulation header. The ToS bits can be set manually or copied from the header of the inner IP packet by issuing the **reflect** keyword.

The ToS bits of the inner IP header can be set manually by using the **set ip tos** (route-map) command. If you then configure the **ip tos reflect** command, the manually configured ToS setting of the inner IP header is copied to the encapsulation header.

The **reflect** keyword functions only when the inner payload is IP. The encapsulated payload of Multilink PPP (MLP) connections is not IP; therefore, the **reflect** keyword has no effect when MLP is tunneled.

The table below shows the format of the four ToS bits in binary form.

Table 4 ToS Bits and Description

T3	T2	T1	T0	Description
0	0	0	0	0 normal forwarding
0	0	0	1	1 minimum monetary cost
0	0	1	0	2 maximum reliability
0	1	0	0	4 maximum throughput
1	0	0	0	8 minimum delay

The T3 bit sets the delay. Setting T3 to 0 equals normal delay, and setting it to 1 equals low delay.

The T2 bit sets the throughput. Setting this bit to 0 equals normal throughput, and setting it to 1 equals maximum throughput. Similarly, the T1 and T0 bits set reliability and monetary cost, respectively. Therefore, as an example, if you want to set a packet with the following requirements:

minimum delay T3 = 1

normal throughput T2 = 0

normal reliability T1 = 0

minimum monetary cost T0 = 1

You would set the ToS to 9, which is 1001 in binary format.

Examples

The following example configures a tunnel server to preserve the IP ToS settings of the encapsulated IP payload for a Layer 2 Tunneling Protocol (L2TP) dial-in sessions:

```
vpdn-group 1
 accept-dialin
  protocol l2tp
  virtual-template 1
 terminate-from hostname router12
 local name router32
 ip tos reflect
```

The following example sets the IP ToS bits to 8 (minimum delay as shown in the table above) for packets that traverse the VPDN tunnel associated with VPDN group 1:

```
vpdn-group 1
 ip tos 8
```

Related Commands

Command	Description
ip precedence	Sets the precedence value (and an optional IP number or IP name) in the VPDN Layer 2 encapsulation header.
set ip tos (route-map)	Sets the ToS bits in the header of an IP packet.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.
vpdn-template	Creates a VPDN template and enters VPDN template configuration mode.