Cisco IOS VPDN Command Reference

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

CONTENTS

A through K

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.

L

l2f ignore-mid-sequence

Note Effective with Cisco Release 12.4(11)T, the **l2f ignore-mid-sequence** command is not available in Cisco IOS software.

To configure the router to ignore multiplex ID (MID) sequence numbers for sessions in a Layer 2 Forwarding (L2F) tunnel, use the **l2f ignore-mid-sequence** command in VPDN group or VPDN template configuration mode. To remove the ability to ignore MID sequencing, use the **no** form of this command.

l2f ignore-mid-sequence

no l2f ignore-mid-sequence

Syntax Description

This command has no arguments or keywords.

Command Default

MID sequence numbers are not ignored.

Command Modes

VPDN group configuration (config-vpdn)

VPDN template configuration (config-vpdn-temp)

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.
12.4(11)T	This command has been removed.

Usage Guidelines

This command applies only to L2F initiated tunnels and control packets for initial link control protocol (LCP) tunnel negotiation.

This command is not required when both tunnel endpoints are Cisco equipment but is required only if MID sequence numbering is not supported by third-party hardware.

Examples

The following example configures the VPDN group named group1 to ignore MID sequencing for L2F sessions between a Cisco router and a non-Cisco hardware device that does not support MID sequencing:

```
vpdn-group group1
 l2f ignore-mid-sequence
```

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.

l2f tunnel busy timeout

Note Effective with Cisco Release 12.4(11)T, the **l2f tunnel busy timeout** command is not available in Cisco IOS software.

To configure the amount of time that the router waits before attempting to recontact a Layer 2 Forwarding (L2F) peer that was previously busy, use the **l2f tunnel busy timeout** command in VPDN group or VPDN template configuration mode. To restore the default value, use the **no** form of this command.

l2f tunnel busy timeout *seconds*

no l2f tunnel busy timeout

Syntax Description

seconds	Time, in seconds, to wait before checking for router availability. The range is 5 to 6000. The default value is 60.

Command Default

The router waits 300 seconds before attempting to recontact a previously busy peer.

Command Modes

VPDN group configuration (config-vpdn)

VPDN template configuration (config-vpdn-temp)

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.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.4(11)T	This command was removed.

Examples

The following example configures the router to leave an L2F peer on the busy list for 90 seconds. This configuration affects only tunnels associated with the virtual private dialup network (VPDN) group named group1.

```
vpdn-group group1
 l2f tunnel busy timeout 90
```

Related Commands

Command	Description
l2f tunnel retransmit initial retries	Configures the number of times that the router attempts to send the initial control packet for tunnel establishment before considering an L2F peer busy.
l2f tunnel retransmit retries	Configures the number of times the router attempts to resend an L2F tunnel control packet before tearing the tunnel down.
l2f tunnel timeout setup	Configures the amount of time that the router waits for a confirmation message after sending the initial L2F control packet before considering a peer busy.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.
vpdn-template	Creates a VPDN template and enters VPDN template configuration mode.

l2f tunnel retransmit initial retries

Note Effective with Cisco Release 12.4(11)T, the **l2f tunnel retransmit initial retries** command is not available in Cisco IOS software.

To configure the number of times that the router attempts to send the initial control packet for tunnel establishment before considering a Layer 2 Forwarding (L2F) peer busy, use the **l2f tunnel retransmit initial retries** command in VPDN group or VPDN template configuration mode. To restore the default value, use the **no** form of this command.

l2f tunnel retransmit initial retries *number*

no l2f tunnel retransmit initial retries

Syntax Description

number	The number of retries that will be attempted. The range is 1 to 1000. The default value is 2.

Command Default

The router sends the initial control packet twice.

Command Modes

VPDN group configuration (config-vpdn)

VPDN template configuration (config-vpdn-temp)

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.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.4(11)T	This command was removed.

Usage Guidelines

This command can be used only if load sharing is enabled.

Examples

The following example configures a dial-in VPDN group on a network access server (NAS) to load balance calls between two tunnel servers and to attempt to send the initial L2F control packet five times:

```
vpdn-group 1
 request-dialin
  protocol l2f
  domain cisco.com
!
 initiate-to ip 172.16.0.1 priority 1
 initiate-to ip 172.16.1.1 priority 2
 l2f tunnel retransmit initial retries 5
```

Related Commands

Command	Description
l2f tunnel busy timeout	Configures the amount of time that the router waits before attempting to recontact an L2F peer that was previously busy.
l2f tunnel retransmit retries	Configures the number of times the router attempts to resend an L2F tunnel control packet before tearing the tunnel down.
l2f tunnel timeout setup	Configures the amount of time that the router waits for a confirmation message after sending the initial L2F control packet before considering a peer busy.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.
vpdn-template	Creates a VPDN template and enters VPDN template configuration mode.

l2f tunnel retransmit retries

Note Effective with Cisco Release 12.4(11)T, the **l2f tunnel retransmit retries** command is not available in Cisco IOS software.

To configure the number of times the router attempts to resend a Layer 2 Forwarding (L2F) tunnel control packet before tearing the tunnel down, use the **l2f tunnel retransmit retries** command in VPDN group or VPDN template configuration mode. To restore the default value, use the **no** form of this command.

l2f tunnel retransmit retries *number*

no l2f tunnel retransmit retries

Syntax Description

number	The number of retries that will be attempted. The range is 5 to 1000. The default value is 6.

Command Default

The router resends control packets six times.

Command Modes

VPDN group configuration (config-vpdn)

VPDN template configuration (config-vpdn-temp)

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.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.4(11)T	This command was removed.

Usage Guidelines

This command does not affect the initial tunnel setup message or session control packets.

Examples

The following example configures the router to resend L2F tunnel control packets ten times before tearing the tunnel down. This configuration affects only tunnels associated with the virtual private dialup network (VPDN) group named group1.

```
vpdn-group group1
 l2f tunnel retransmit retries 10
```

Related Commands

Command	Description
l2f tunnel busy timeout	Configures the amount of time that the router waits before attempting to recontact an L2F peer that was previously busy.
l2f tunnel retransmit initial retries	Configures the number of times that the router attempts to send the initial control packet for tunnel establishment before considering an L2F peer busy.
l2f tunnel timeout setup	Configures the amount of time that the router waits for a confirmation message after sending the initial L2F control packet before considering a peer busy.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.
vpdn-template	Creates a VPDN template and enters VPDN template configuration mode.

l2f tunnel timeout setup

Note

Effective with Cisco Release 12.4(11)T, the **l2f tunnel timeout setup** command is not available in Cisco IOS software.

To configure the amount of time that the router waits for a confirmation message after sending the initial Layer 2 Forwarding (L2F) control packet before considering a peer busy, use the **l2f tunnel timeout setup** command in VPDN group or VPDN template configuration mode. To restore the default value, use the **no** form of this command.

l2f tunnel timeout setup *seconds*

no l2f tunnel timeout setup

Syntax Description

seconds	Time, in seconds, that the router will wait for a return message. The range is 5 to 6000. The default value is 10.

Command Default

The router waits 10 seconds for a confirmation message.

Command Modes

VPDN group configuration (config-vpdn)

VPDN template configuration (config-vpdn-temp)

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.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.4(11)T	This command was removed.

Usage Guidelines

If the router does not receive a confirmation message from the peer device before the tunnel timeout setup timer expires, the peer is placed on the busy list.

Examples

The following example configures a router to wait 25 seconds for confirmation that the initial L2F control packet was received by the peer. This configuration affects only tunnels associated with the virtual private dialup network (VPDN) group named group1.

```
vpdn-group group1
 l2f tunnel timeout setup 25
```

Related Commands

Command	Description
l2f tunnel busy timeout	Configures the amount of time that the router waits before attempting to recontact an L2F peer that was previously busy.
l2f tunnel retransmit initial retries	Configures the number of times that the router attempts to send the initial control packet for tunnel establishment before considering an L2F peer busy.
l2f tunnel retransmit retries	Configures the number of times the router attempts to resend an L2F tunnel control packet before tearing the tunnel down.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.
vpdn-template	Creates a VPDN template and enters VPDN template configuration mode.

l2tp attribute clid mask-method

To configure a network access server (NAS) to suppress Layer 2 Tunneling Protocol (L2TP) calling station IDs for sessions associated with a virtual private dialup network (VPDN) group or VPDN template, use the **l2tp attribute clid mask-method** command in VPDN group or VPDN template configuration mode. To disable L2TP calling station ID suppression, use the **no** form of this command.

l2tp attribute clid mask-method {**right** *mask-character characters* | **remove**} [**match** *match-string*]

no l2tp attribute clid mask-method {**right** *mask-character characters* | **remove**} [**match** *match-string*]

Syntax Description

right	Specifies that the calling station ID will be masked by replacing characters, starting from the right end of the string.
mask-character	Character to be used as a replacement. Only printable characters are accepted.
characters	Number of characters to be replaced.
remove	Specifies that the entire calling station ID will be removed.
match *match-string*	(Optional) Applies the defined masking method only if the string specified by the *match-string* argument is contained in the username.

Command Default

The calling station ID is not masked or dropped.

Command Modes

VPDN group configuration (config-vpdn)
VPDN template configuration (config-vpdn-temp)

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.3(14)YM2	This command was integrated into Cisco IOS Release 12.3(14)YM2 and implemented on the Cisco 7301, Cisco 7204VXR, and Cisco 7206VXR routers.

Usage Guidelines

The **l2tp attribute clid mask-method** command can be used to mask the calling station ID in L2TP attribute-value (AV) pair 22. This command is compatible with only local authorization. You can either substitute characters for a portion of the calling station ID or remove the entire calling station ID.

Use the **l2tp attribute clid mask-method** command in VPDN group configuration mode to mask the calling station ID for calls belonging to that VPDN group.

Use the **l2tp attribute clid mask-method** command in VPDN template configuration mode to mask the calling station ID for calls belonging to any VPDN group associated with that VPDN template.

The **vpdn l2tp attribute clid mask-method** command masks the calling station ID globally for all VPDN groups configured on the NAS and is compatible with both local and remote RADIUS AAA authorization.

Examples

The following example shows how to use the **l2tp attribute clid mask-method** command to remove the calling station ID during local authorization if the username contains the string #184. This configuration applies only to calls belonging to the VPDN group named l2tp.

```
vpdn-group l2tp
 request-dialin
  protocol l2tp
  domain cisco.com
  domain cisco.com#184
!
 initiate-to ip 10.168.1.4
 local name router32
 l2tp tunnel password 0 cisco
 l2tp attribute clid mask-method remove match #184
```

Related Commands

Command	Description
vpdn l2tp attribute clid mask-method	Configures a NAS to suppress L2TP calling station IDs globally on the router.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.
vpdn-template	Creates a VPDN template and enters VPDN template configuration mode.

l2tp congestion-control

To enable Layer 2 Tunneling Protocol (L2TP) congestion avoidance, use the **l2tp congestion-control** command in global configuration mode. To disable L2TP congestion avoidance, use the **no** form of this command.

l2tp congestion-control

no l2tp congestion-control

Syntax Description

This command has no arguments or keywords.

Command Default

L2TP congestion avoidance is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(28)SB	This command was introduced.
15.0(1)M	This command was integrated into a release earlier than Cisco IOS Release 15.0(1)M.

Usage Guidelines

The **l2tp congestion-control** command operates as a user-controlled on-off switch. An L2TP sliding window mechanism is enabled or disabled by this command. The **l2tp congestion-control** command is enabled by default, and congestion control is enabled on any existing virtual private dialup network (VPDN) tunnel. To disable congestion control, use the **no** form of the command.

The congestion window size is not allowed to exceed the size of the advertised window obtained from the receive window size set by the **l2tp tunnel receive-window** VPDN group configuration command. Lowering the value of the receive window results in lowering the number of calls per second being negotiated, and if a network is congested, the receive window size should be lowered. Increasing this value depends on how congested the network is. When the network becomes less congested, the receive window size can be increased again.

Examples

The following example enables L2TP congestion avoidance:

```
Router(config)# l2tp congestion-control
```

Related Commands

Command	Description
l2tp tunnel receive-window	Specifies the size of the advertised receive window.

l2tp drop out-of-order

To instruct a network access server (NAS) or tunnel server using Layer 2 Tunneling Protocol (L2TP) to drop packets that are received out of order, use the **l2tp drop out-of-order** command in VPDN group or VPDN template configuration mode. To disable dropping of out-of-sequence packets, use the **no** form of this command.

l2tp drop out-of-order

no l2tp drop out-of-order

Syntax Description

This command has no arguments or keywords.

Command Default

Out of order packets are not dropped.

Command Modes

VPDN group configuration (config-vpdn)

VPDN template configuration (config-vpdn-temp)

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.

Usage Guidelines

This command is valid only for tunnels where sequencing is enabled.

Examples

The following example enables sequencing and configures the router to drop any out-of-order packets that are received on a tunnel associated with the VPDN group named tunnelme:

```
vpdn-group tunnelme
 l2tp sequencing
 l2tp drop out-of-order
```

Related Commands

Command	Description
l2tp sequencing	Enables sequencing for packets sent over an L2TP tunnel.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.
vpdn-template	Creates a VPDN template and enters VPDN template configuration mode.

l2tp hidden

To enable Layer 2 Tunneling Protocol (L2TP) attribute-value (AV) pair hiding, which encrypts the value of sensitive AV pairs, use the **l2tp hidden** command in VPDN group or VPDN template configuration mode. To disable L2TP AV pair value hiding, use the **no** form of this command.

l2tp hidden

no l2tp hidden

Syntax Description

This command has no arguments or keywords.

Command Default

L2TP AV pair hiding is disabled.

Command Modes

VPDN group configuration (config-vpdn)

VPDN template configuration (config-vpdn-temp)

Command History

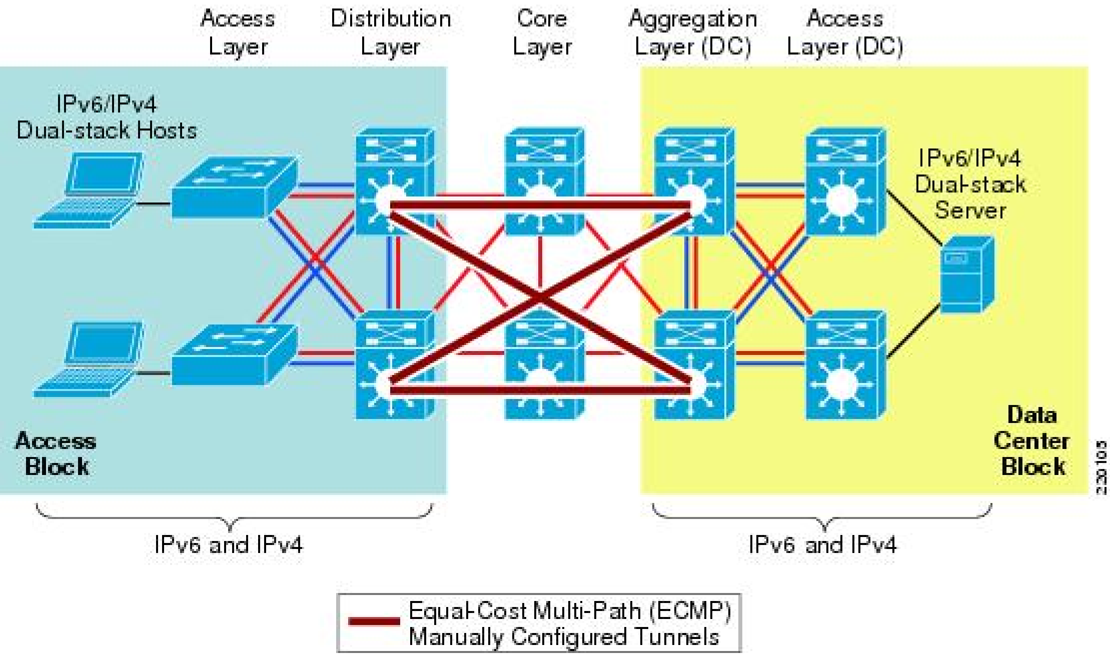
Release	Modification
11.3(5)AA	This command was introduced.
12.0(1)T	This command was integrated into Cisco IOS Release 12.0(1)T.

Usage Guidelines

This command is not required if one-time Password Authentication Protocol (PAP) password authentication is used. This command is useful for additional security if PPP is using PAP or proxy authentication between the L2TP access concentrator (LAC) and L2TP network server (LNS). When AV pair hiding is enabled, the L2TP hiding algorithm is executed, and sensitive passwords that are used between the L2TP AV pairs are encrypted during PAP or proxy authentication.

In the figure below, the client initiates a PPP session with the LAC, and tunnel authentication begins. The LAC in turn exchanges authentication requests with the LNS. Upon successful authentication between the LAC and LNS, a tunnel is created. Proxy authentication is performed by the LAC using either PAP or Challenge Handshake Authentication Protocol (CHAP). Because PAP username and password information is exchanged between devices in clear-text, use the **l2tp hidden** command where L2TP AV pair values are encrypted.

Figure 1 LAC-LNS Proxy Authentication



Examples

The following example encrypts the AV pair value exchanged between the endpoints of tunnels associated with the VPDN group named group1:

```
vpdn-group group1
 l2tp hidden
```

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.

l2tp ip udp checksum

To enable IP User Data Protocol (UDP) checksums on Layer 2 Tunneling Protocol (L2TP) data packets, use the **l2tp ip udp checksum** command in VPDN group or VPDN template configuration mode. To disable IP UDP checksums, use the **no** form of this command.

l2tp ip udp checksum

no l2tp ip udp checksum

Syntax Description

This command has no arguments or keywords.

Command Default

UDP checksums are not used on L2TP data packets.

Command Modes

VPDN group configuration (config-vpdn)

VPDN template configuration (config-vpdn-temp)

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.

Usage Guidelines

Enabling IP UDP checksums on data packets causes the switching path to revert to process-level switching, which results in slower performance. The drop in performance might be acceptable if the connection between the network access server (NAS) and the tunnel server is poor. Enabling IP UDP checksums minimizes delays that occur when the ultimate error correction is done end-to-end rather than at the tunnel endpoints.

Examples

The following example enables IP UDP checksums on L2TP data packets for tunnels associated with the virtual private dialup network (VPDN) group named group1:

```
vpdn-group group1
 l2tp ip udp checksum
```

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.

l2tp rx-speed

To configure the receive-speed (rx-speed) value for Layer 2 Tunneling Protocol (L2TP) to be sent to L2TP network server (LNS), use the **l2tp rx-speed** command in VPDN group configuration or VPDN template configuration mode. To return the default value, use the **no** form of this command.

l2tp rx-speed {*value* | **ancp** [*value*] | **ram-min** [*value*]}

no l2tp rx-speed {*value* | **ancp** [*value*] | **ram-min** [*value*]}

Syntax Description

ancp	Specifies that the source to obtain the rx-speed value is Access Node Control Protocol (ANCP).
ram-min	Specifies that the source to obtain the rx-speed value is Rate Adaptive Mode-minimum (RAM-min).
value	(Optional) The rx-speed value in kilobits per second (kbps). The range is 0 to 2147483.

Command Default

L2TP obtains the rx-speed value from Point-to-Point Protocol over Ethernet (PPPoE) and sends it to the LNS.

Command Modes

VPDN group configuration (config-vpdn)

VPDN template configuration (config-vpdn-temp)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines

Use the **l2tp rx-speed** command to configure the rx-speed value that the L2TP sends to the LNS.

- If the source specified is ANCP, L2TP sends the upstream value configured for ANCP to the LNS.
- If the source specified is RAM-min, L2TP sends the rx-speed value configured for RAM-min to the LNS.
- If the rx-speed is not configured for ANCP or RAM-min, L2TP sends the rx-speed value specified in the command.

Examples

The following example shows how to configure the rx-speed value locally:

```
Router(config)# vpdn-group 1
Router(config-vpdn)# l2tp rx-speed 8000
```

The following example shows how to configure L2TP to obtain the rx-speed value from ANCP, and if rx-speed is not configured for ANCP, L2TP sends the locally configured rx-speed value to the LNS:

```
Router(config)# vpdn-template 2
Router(config-vpdn-temp)# l2tp rx-speed ancp 15000
```

The following example shows how to configure L2TP to obtain the rx-speed value from RAM-min, and if rx-speed is not configured for RAM-min, L2TP sends the locally configured rx-speed value to the LNS:

```
Router(config)# vpdn-group 1
Router(config-vpdn)# l2tp rx-speed ram-min 10000
```

Related Commands

Command	Description
l2tp tx-speed	Configures the tx-speed value to be sent to the LNS.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.
vpdn-template	Creates a VPDN template and enters VPDN template configuration mode.

l2tp security crypto-profile

To configure IP Security (IPSec) protection of Layer 2 Tunneling Protocol (L2TP) sessions associated with a virtual private dialup network (VPDN) group, use the **l2tp security crypto-profile** command in VPDN group or VPDN template configuration mode. To disable IPSec protection for a VPDN group, use the **no** form of this command.

l2tp security crypto-profile *profile-name* [**keep-sa**]

no l2tp security crypto-profile

Syntax Description

profile-name	The name of the crypto profile to be used for IPSec protection of tunneled PPP sessions.
keep-sa	(Optional) Controls the destruction of IPSec security associations (SAs) upon tunnel teardown. By default, any IPSec phase 2 SAs and Internet Key Exchange (IKE) phase 1 SAs are destroyed when the L2TP tunnel is torn down. Issuing the **keep-sa** keyword prevents the destruction of IKE phase 1 SAs.

Command Default

IPSec security is disabled. IKE phase 1 SAs are destroyed on tunnel teardown.

Command Modes

VPDN group configuration (config-vpdn)

VPDN template configuration (config-vpdn-temp)

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

Usage Guidelines

Enabling this command for a VPDN group ensures that no L2TP packets are processed unless they have IPSec protection.

A crypto profile must be configured by using the **crypto map** (global IPSec) command before it can be associated with a VPDN group with the **l2tp security crypto-profile** command. The *profile-name* argument must match the name of a profile configured through the **crypto map** command.

The **keep-sa** keyword can be used to prevent the destruction of IKE phase 1 SAs when the L2TP tunnel between the network access server (NAS) and tunnel server is considered permanent, and the IP addresses of the peer devices rarely change. This option is not useful with short-lived tunnels, such as those generated by client-initiated L2TP tunneling.

Examples

The following example configures VPDN group 1, associates it with the crypto profile named l2tp, and prevents the destruction of IKE phase 1 SAs on tunnel teardown:

```
vpdn-group 1
 request-dialin
  protocol l2tp
  domain cisco.com
 initiate-to ip 10.0.0.13
 local name LAC
 l2tp security crypto-profile l2tp keep-sa
```

Related Commands

Command	Description
crypto map (global IPSec)	Enters crypto map configuration mode and creates or modifies a crypto map entry, creates a crypto profile that provides a template for configuration of dynamically created crypto maps, or configures a client accounting list.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.
vpdn-template	Creates a VPDN template and enters VPDN template configuration mode.

l2tp security ip address-check

To enable the checking of an IP address from an Layer 2 Tunneling Protocol (L2TP) network server (LNS) before the setup of an L2TP tunnel from the L2TP Access Concentrator (LAC) to the LNS, use the **l2tp security ip address-check** command in VPDN group configuration mode. To disable the checking of an IP address from an LNS before the setup of an L2TP tunnel from the LAC to the LNS, use the **no** form of this command.

l2tp security ip address-check

no l2tp security ip address-check

Syntax Description

This command has no arguments or keywords.

Command Default

The command is disabled.

Command Modes

VPDN-group configuration (config-vpdn)

Command History

Release	Modification
12.2(31)ZV	This command was introduced.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

You can configure the **l2tp security ip address-check** command only on a LAC; this command is not accepted on an LNS.

Use the **l2tp security ip address-check** command to enable or disable the matching, prior to an L2TP tunnel setup of an incoming transport IP address from a LNS against the output IP address of the LNS by the LAC. Once enabled, the LAC inspects, prior to establishing an L2TP tunnel if the IP addresses contained in the Start Control Connection Reply (SCCRP) and Start Control Connection Request (SCCRQ) messages, are identical. If these IP addresses do not match, an L2TP tunnel is not established.

You cannot configure the **l2tp security ip address-check** command on a VPDN group that has the **accept-dialin** command configured.

You can use the **debug vpdn 12x-error** command with the **l2tp security ip address-check** command to display informational messages on each control packet dropped.

Examples

The following example shows how to enable the verification of an incoming transport IP address from an LNS against the output IP address of the LNS:

```
LAC> enable

LAC# configure terminal
LAC(config)# vpdn enable
LAC(config)# vpdn-group example
LAC(config-vpdn)# l2tp security ip address-check
```

Related Commands

Command	Description
debug vpdn 12x-error	Displays a message for each control packet dropped.

l2tp sequencing

To enable sequencing for packets sent over a Layer 2 Tunneling Protocol (L2TP) tunnel, use the **l2tp sequencing** command in VPDN group or VPDN template configuration mode. To disable sequencing, use the **no** form of this command.

l2tp sequencing

no l2tp sequencing

Syntax Description

This command has no arguments or keywords.

Command Default

Sequencing is disabled by default. However, if the peer device requests sequencing, it will be enabled.

Command Modes

VPDN group configuration (config-vpdn)

VPDN template configuration (config-vpdn-temp)

Command History

Release	Modification
12.1	This command was introduced.

Usage Guidelines

Use the **l2tp sequencing** command to control sequencing for packets sent over an L2TP tunnel.

The **l2tp sequencing** command configuration might be overridden by a request for sequencing from the peer device. The following sections describe the default behavior and sequencing request interactions of the two tunnel endpoints.

Tunnel Initiator

- By default, sequence numbers are off.
- By default, the Sequencing Required attribute-value (AV) pair is not sent from the tunnel initiator to the tunnel terminator.
- If the tunnel initiator receives data packets from the tunnel terminator that include sequencing numbers, the tunnel initiator includes sequence numbers on data packets regardless of the **l2tp sequencing** command configuration.
- Enabling the **l2tp sequencing** command causes the tunnel initiator to send the Sequencing Required AV pair to the tunnel terminator and to include sequencing numbers on data packets.

Tunnel Terminator

- By default, sequence numbers are off.

- If the tunnel terminator receives the Sequencing Required AV pair from the tunnel initiator, the tunnel terminator includes sequence numbers on data packets regardless of the **l2tp sequencing** command configuration.
- Enabling the **l2tp sequencing** command causes the tunnel terminator to include sequence numbers.

Examples

The following example configures sequencing on a network access server (NAS) for dial-in L2TP tunnels associated with the VPDN group named tunnelme. The NAS sends the Sequencing Required AV pair to the tunnel server, and sequencing is enabled on both devices.

```
vpdn-group tunnelme
 request-dialin
  protocol l2tp
  domain cisco.com
!
 local name router32
 initiate to 172.16.1.1
 l2tp sequencing
```

Related Commands

Command	Description
l2tp drop out-of-order	Instructs a NAS or tunnel server using L2TP to drop packets that are received out of order.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.
vpdn-template	Creates a VPDN template and enters VPDN template configuration mode.

l2tp sso enable

To enable the Layer 2 Tunneling Protocol (L2TP) high availability (HA) feature, use the **l2tp sso enable** command in global configuration mode. To disable the L2TP HA feature, use the **no** form of this command.

l2tp sso enable

no l2tp sso enable

Syntax Description

This command has no arguments or keywords.

Command Default

L2TP SSO is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 2.2.	This command was introduced.

Usage Guidelines

This command is enabled by default and is hidden from the output of the **show running-config** command.

Use the **no l2tp sso enable** command to disable L2TP HA globally and for any virtual private dial-in network (VPDN) group previously enabled by using the **sso enable** command. If you disable L2TP HA, the **l2tp sso enable** command displays as NVGEN in the output of the **show running-config** command.

Use the **debug l2tp redundancy** and the **debug vpdn redundancy** commands in privileged EXEC mode to display a list L2TP HA checkpointed events and errors.

Use the **show l2tp redundancy** command in privileged EXEC mode to display L2TP checkpointed status information.

Examples

The following example shows how to globally disable L2TP HA functionality for all VPDN groups:

```
Router> configure terminal
Router(config)# no l2tp sso enable
```

Related Commands

Command	Description
debug l2tp redundancy	Displays information on L2TP sessions having redundancy events and errors.
debug vpdn redundancy	Displays information on VPDN sessions having redundancy events and errors.
l2tp tunnel resync	Specifies the number of packets sent before waiting for an acknowledgment message.
show l2tp redundancy	Displays L2TP sessions containing redundancy data.
show vpdn redundancy	Displays VPDN sessions containing redundancy data.
sso enable	Enables L2TP HA for VPDN groups.

l2tp tunnel authentication

To enable Layer 2 Tunneling Protocol (L2TP) tunnel authentication, use the **l2tp tunnel authentication** command in VPDN group or VPDN template configuration mode. To disable L2TP tunnel authentication, use the **no** form of this command.

l2tp tunnel authentication

no l2tp tunnel authentication

Syntax Description

This command has no arguments or keywords.

Command Default

L2TP tunnel authentication is enabled.

Command Modes

VPDN group configuration (config-vpdn)

VPDN template configuration (config-vpdn-temp)

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.

Examples

The following example disables L2TP tunnel authentication for tunnels associated with the virtual private dialup network (VPDN) group named group1:

```
vpdn-group group1
 no l2tp tunnel authentication
```

The following example reenables L2TP tunnel authentication for tunnels associated with the VPDN group named group1:

```
vpdn-group group1
 l2tp tunnel authentication
```

Note L2TP tunnel authentication is enabled by default so there is no need to enable this command unless it was previously disabled.

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.

l2tp tunnel bearer capabilities

To set the Layer 2 Tunneling Protocol (L2TP) bearer-capability value used by the Cisco router, use the **l2tp tunnel bearer capabilities** command in VPDN group or VPDN template configuration mode. To restore the default value, use the **no** form of this command.

l2tp tunnel bearer capabilities {**none** | **digital** | **analog** | **all**}

no l2tp tunnel bearer capabilities

Syntax Description

none	Specifies that no access types are supported. This is the default value if the **accept-dialout** command is not configured..
digital	Specifies that digital access is supported.
analog	Specifies that analog access is supported.
all	Specifies that all access types are supported. This is the default value if the **accept-dialout** command is configured.

Command Default

If the **accept-dialout** command is not configured, no access types are supported. If the **accept-dialout** command is configured, all access types are supported.

Command Modes

VPDN group configuration (config-vpdn)

VPDN template configuration (config-vpdn-temp)

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

By default, Cisco routers use a bearer-capability value of **none**. If the **accept-dialout** command is configured, Cisco routers use a bearer-capability value of **all**. To ensure compatibility with some non-Cisco routers, you might be required to override the default bearer-capability value by configuring the **l2tp tunnel bearer capabilities** command.

Examples

The following example configures the bearer-capability value to support only digital access for tunnels associated with the virtual private dialup network (VPDN) group named group1:

```
vpdn-group group1
 l2tp tunnel bearer capabilities digital
```

Related Commands

Command	Description
accept-dialout	Accepts requests to tunnel L2TP dial-out calls and creates an accept-dialout VPDN subgroup.
l2tp tunnel framing capabilities	Sets the framing-capability value used by the Cisco router.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.
vpdn-template	Creates a VPDN template and enters VPDN template configuration mode.

l2tp tunnel busy timeout

To configure the amount of time that the router waits before attempting to recontact a Layer 2 Tunneling Protocol (L2TP) peer that was previously busy, use the **l2tp tunnel busy timeout** command in VPDN group or VPDN template configuration mode. To restore the default value, use the **no** form of this command.

l2tp tunnel busy timeout *seconds*

no l2tp tunnel busy timeout

Syntax Description

seconds	Time, in seconds, to wait before checking for router availability. The range is 5 to 6000. The default value is 60.

Command Default

The router waits 300 seconds before attempting to recontact a previously busy peer.

Command Modes

VPDN group configuration (config-vpdn)

VPDN template configuration (config-vpdn-temp)

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

Examples

The following example configures tunnels associated with the virtual private dialup network (VPDN) group named group1 to leave an L2TP destination router on the busy list for 90 seconds:

```
vpdn-group group1
 l2tp tunnel busy timeout 90
```

Related Commands

Command	Description
l2tp tunnel retransmit initial retries	Sets the number of times that the router attempts to send the initial control packet for tunnel establishment before considering a router busy.
l2tp tunnel retransmit initial timeout	Sets the amount of time that the router waits before resending an initial packet out to establish a tunnel.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.
vpdn-template	Creates a VPDN template and enters VPDN template configuration mode.

l2tp tunnel framing capabilities

To set the Layer 2 Tunneling Protocol (L2TP) framing-capability value used by the Cisco router, use the **l2tp tunnel framing capabilities** command in VPDN group or VPDN template configuration mode. To restore the default value, use the **no** form of this command.

l2tp tunnel framing capabilities {**none** | **synchronous** | **asynchronous** | **all**}

no l2tp tunnel framing capabilities

Syntax Description

none	Specifies that no framing types are supported. This is the default value if the **accept-dialout** command is not configured.
synchronous	Specifies that synchronous framing is supported.
asynchronous	Specifies that asynchronous framing is supported.
all	Specifies that all framing types are supported. This is the default value if the **accept-dialout** command is configured.

Command Default

If the **accept-dialout** command is not configured, no framing types are supported. If the **accept-dialout** command is configured, all framing types are supported.

Command Modes

VPDN group configuration (config-vpdn)

VPDN template configuration (config-vpdn-temp)

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

By default, Cisco routers use a framing-capability value of **none**. If the **accept-dialout** command is configured, Cisco routers use a framing-capability value of **all**. To ensure compatibility with some non-Cisco routers, you might be required to override the default framing-capability value by configuring the **l2tp tunnel framing capabilities** command.

Examples

The following example configures the framing-capability value to support only asynchronous framing for tunnels associated with the virtual private dialup network (VPDN) group named group1:

```
vpdn-group group1
 l2tp tunnel framing capabilities asynchronous
```

Related Commands

Command	Description
accept-dialout	Accepts requests to tunnel L2TP dial-out calls and creates an accept-dialout VPDN subgroup.
l2tp tunnel bearer capabilities	Sets the bearer-capability value used by the Cisco router.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.
vpdn-template	Creates a VPDN template and enters VPDN template configuration mode.

l2tp tunnel hello

To set the number of seconds between sending hello keepalive packets for a Layer 2 Tunneling Protocol (L2TP) tunnel, use the **l2tp tunnel hello** command in virtual private dialup network (VPDN) group or VPDN template configuration mode. To return to the default setting, use the **no** form of this command.

l2tp tunnel hello *seconds*

no l2tp tunnel hello

Syntax Description

seconds	The interval, in seconds, that the network access server (NAS) and tunnel server wait before sending the next L2TP tunnel keepalive packet. The range is 0 to 1000. The default value is 60.

Command Default

Hello keepalive packets are sent every 60 seconds.

Command Modes

VPDN group configuration (config-vpdn)

VPDN template configuration (config-vpdn-temp)

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.

Usage Guidelines

To change the tunnel hello value, reenter the command with the new value.

The L2TP tunnel keepalive timers need not use the same value on both sides of the tunnel. For example, a NAS can use a keepalive value of 30 seconds, and a tunnel server can use the default value of 60 seconds.

Note

We do not recommend setting the **l2tp tunnel hello** command to zero seconds. Disabling the sending of L2TP tunnel hello messages can prevent the NAS or tunnel server from tearing down a tunnel and cleaning up a half-open session if the connection with the peer becomes stuck. The NAS or tunnel server sends hello packets only if it does not receive packets from the peer over the tunnel for 60 seconds (or the configured value). In a normal connection, hello packets are not sent; they are sent only if the connection becomes stuck.

Examples

The following example sets the L2TP tunnel hello value to 90 seconds for tunnels associated with the VPDN group named group1:

```
vpdn-group group1
 l2tp tunnel hello 90
```

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.

l2tp tunnel password

To set the password that the router uses to authenticate Layer 2 Tunneling Protocol (L2TP) tunnels, use the **l2tp tunnel password** command in VPDN group or VPDN template configuration mode. To remove a previously configured password, use the **no** form of this command.

l2tp tunnel password *password*

no l2tp tunnel password

Syntax Description

password	String that the router uses for tunnel authentication.

Command Default

The password associated with the local name of the router is used to authenticate the tunnel. If no local name password is configured, the password associated with the hostname of the router is used to authenticate the tunnel.

Command Modes

VPDN group configuration (config-vpdn)

VPDN template configuration (config-vpdn-temp)

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.

Usage Guidelines

The password defined with the **l2tp tunnel password** command is also used for attribute-value (AV) pair hiding.

The password hierarchy sequence that is used for tunnel identification, and subsequently tunnel authentication, is as follows:

- An L2TP tunnel password is used if one is configured.
- If no L2TP tunnel password exists, the password associated with the local name of the router is used.
- If a local name password does not exist, the password associated with the hostname of the router is used.

The **username** command is used to define the passwords associated with the local name and the hostname.

Examples

The following example configures the L2TP tunnel password, *secret*, which is used to authenticate tunnels associated with the virtual private dialup network (VPDN) group named group1:

```
vpdn-group group1
 l2tp tunnel password secret
```

Related Commands

Command	Description
hostname	Specifies or modifies the hostname for the network server.
l2tp hidden	Enables L2TP AV pair hiding, which encrypts the value of sensitive AV pairs.
local name	Specifies a local hostname that the tunnel uses to identify itself.
username	Establishes a username-based authentication system.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.
vpdn-template	Creates a VPDN template and enters VPDN template configuration mode.

l2tp tunnel receive-window

To configure the number of packets allowed in the local receive window for a Layer 2 Tunneling Protocol (L2TP) control channel, use the **l2tp tunnel receive-window** command in VPDN group configuration or VPDN template configuration mode. To restore the default value, use the **no** form of this command.

l2tp tunnel receive-window *packets*

no l2tp tunnel receive-window

Syntax Description

packets	Number of packets allowed in the receive window. The range is 1 to 5000. The default value varies by platform.

Command Default

The default size of the control channel receive window is platform-dependent.

Command Modes

VPDN group configuration (config-vpdn)

VPDN template configuration (config-vpdn-temp)

Command History

Release	Modification
12.0(7)DC	This command was introduced on the Cisco 6400 node route processor (NRP).
12.1(1)	This command was integrated into Cisco IOS Release 12.1(1).
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

Use the **l2tp tunnel receive-window** command to set the size of the advertised control channel receive window. The receive window size controls the number of L2TP control packets that can be queued by the system for processing. Increasing the size of the control channel receive window allows the system to open PPP sessions more quickly; a smaller size is desirable on networks that cannot handle large bursts of traffic.

Cisco 10000 Series Router

We recommend that you configure the L2TP tunnel receive window to 100 packets on the Cisco 10000 series router.

Examples

The following example configures the receive window to hold up to 500 packets for tunnels associated with the virtual private dialup network (VPDN) group named group1:

```
vpdn-group group1
 l2tp tunnel receive-window 500
```

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.

l2tp tunnel resync

To control the number of packets after a stateful switchover (SSO), a Layer 2 Tunneling Protocol (L2TP) high availability (HA) tunnel sends before waiting for an acknowledgment, use the **l2tp tunnel resync** command in VPDN group configuration mode. To disable the control of packets sent, use the **no** form of this command.

l2tp tunnel resync *packets*

no l2tp tunnel resync

Syntax Description

packets	The number of unacknowledged packets sent to the peer for stateful switchover (SSO). The range is 1 to 1024 packets.

Command Default

This command is disabled

Command Modes

VPDN group configuration (config-vpdn)

Command History

Release	Modification
Cisco IOS XE Release 2.2.	This command was introduced in Cisco IOS XE Release 2.2.

Usage Guidelines

Use the **l2tp tunnel resync** command in VPDN group configuration mode to control the number of unacknowledged messages sent to a peer router during SSO.

Use the **show l2tp redundancy** command in privileged EXEC mode to display information on the state of the L2TP or a specific L2TP redundancy session.

Examples

The following example shows setting the L2TP resync packet value to 100 packets:

```
Router> enable
Router# configure terminal
Router(conf)# vpdn enable
Router(conf-vpdn)# vpdn-group example
Router(conf-vpdn)# l2tp tunnel resync 100
Router(conf-vpdn)# exit
```

Related Commands

Command	Description
debug l2tp redundancy	Displays information on L2TP sessions having redundancy events and errors.
debug vpdn redundancy	Displays information on VPDN sessions having redundancy events and errors.
l2tp sso enable	Enables the L2TP HA feature.
show l2tp redundancy	Displays L2TP sessions containing redundancy data.
show vpdn redundancy	Displays VPDN sessions containing redundancy data.
sso enable	Enables L2TP HA for VPDN groups.

l2tp tunnel retransmit initial retries

To configure the number of times that the router attempts to send out the initial Layer 2 Tunneling Protocol (L2TP) control packet for tunnel establishment before considering a peer busy, use the **l2tp tunnel retransmit initial retries** command in VPDN group or VPDN template configuration mode. To restore the default value, use the **no** form of this command.

l2tp tunnel retransmit initial retries *number*

no l2tp tunnel retransmit initial retries

Syntax Description

number	Number of retransmission attempts. The range is 1 to 1000. The default is 2.

Command Default

The router resends the initial L2TP control packet twice.

Command Modes

VPDN group configuration (config-vpdn)
VPDN template configuration (config-vpdn-temp)

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

Usage Guidelines

Use the **l2tp tunnel retransmits initial retries** command to configure the number of times a device attempts to resend the initial control packet used to establish an L2TP tunnel.

Examples

The following example configures the router to attempt to send the initial L2TP control packet five times for tunnels associated with the virtual private dialup network (VPDN) group named group1:

```
vpdn-group group1
 l2tp tunnel retransmit initial retries 5
```

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 timeout	Configures the amount of time that the router waits before resending an initial L2TP control packet out to establish a tunnel.
l2tp tunnel retransmit retries	Configures the number of retransmission attempts made for a L2TP control packet.
l2tp tunnel retransmit timeout	Configures the amount of time that the router waits before resending an L2TP control 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.

l2tp tunnel retransmit initial timeout

To configure the amount of time that the router waits before resending an initial Layer 2 Tunneling Protocol (L2TP) control packet to establish a tunnel, use the **l2tp tunnel retransmit initial timeout** command in VPDN group or VPDN template configuration mode. To restore the default value, use the **no** form of this command.

l2tp tunnel retransmit initial timeout {**min** | **max**} *seconds*

no l2tp tunnel retransmit initial timeout {**min** | **max**}

Syntax Description

min	Specifies the minimum time that the router waits before resending an initial packet.
max	Specifies the maximum time that the router waits before resending an initial packet.
seconds	Timeout length, in seconds, the router waits before resending an initial packet. The range is 1 to 8. The default minimum value is 1. The default maximum value is 8.

Command Default

The minimum timeout is one second. The maximum timeout is eight seconds.

Command Modes

VPDN group configuration (config-vpdn)

VPDN template configuration (config-vpdn-temp)

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

Usage Guidelines

This command takes effect only when load balancing is enabled.

Control channel retransmissions follow an exponential backoff, starting at the minimum retransmit timeout length specified by the **min** *seconds* keyword and argument. After each packet that is not acknowledged, the timeout exponentially increases until it reaches the value specified by the **max** *seconds* keyword and argument. For example, if the minimum timeout length is set to one second, the next retransmission attempt occurs two seconds later. The following attempt occurs four seconds later, and all additional attempts occur in eight second intervals.

Examples

The following example configures a network access server (NAS) virtual private dialup network (VPDN) group to establish L2TP tunnels that are load balanced across two tunnel servers. The NAS is configured to attempt to recontact a peer with an initial control packet five times before considering it busy. The timers are set so that the first attempt to recontact the peer occurs two seconds after the initial failure, and the final attempt occurs seven seconds after the previous failure.

```
vpdn-group 1
 request-dialin
  protocol l2tp
  domain cisco.com
!
 initiate-to ip 172.16.0.1 priority 1
 initiate-to ip 172.16.1.1 priority 2
 l2tp tunnel retransmit initial retries 5
 l2tp tunnel retransmit initial timeout min 2
 l2tp tunnel retransmit initial timeout max 7
```

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	Configures the number of times that the router attempts to send the initial L2TP control packet for tunnel establishment before considering a peer busy.
l2tp tunnel retransmit retries	Configures the number of retransmission attempts made for an L2TP control packet.
l2tp tunnel retransmit timeout	Configures the amount of time that the router waits before resending an L2TP control 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.

l2tp tunnel retransmit retries

To configure the number of retransmission attempts made for a Layer 2 Tunneling Protocol (L2TP) control packet, use the **l2tp tunnel retransmit retries** command in VPDN group or VPDN template configuration mode. To restore the default value, use the **no** form of this command.

l2tp tunnel retransmit retries *number*

no l2tp tunnel retransmit retries *number*

Syntax Description

number	Number of retransmission attempts. The range is 5 to 1000 retries. The default is 10.

Command Default

The router resends control packets ten times.

Command Modes

VPDN group configuration (config-vpdn)

VPDN template configuration (config-vpdn-temp)

Command History

Release	Modification
12.0(7)DC	This command was introduced on the Cisco 6400 node route processor (NRP).
12.1(1)	This command was integrated into Cisco IOS Release 12.1(1).

Usage Guidelines

Use the **l2tp tunnel retransmits retries** command to configure the number of times a device attempts to resend an L2TP control packet.

Examples

The following example tunnels associated with the virtual private dialup network (VPDN) group named group1 to make eight retransmission attempts:

```
vpdn-group group1
 l2tp tunnel retransmit retries 8
```

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	Configures the number of times that the router attempts to send the initial L2TP control packet for tunnel establishment before considering a peer busy.
l2tp tunnel retransmit initial timeout	Configures the amount of time that the router waits before resending an initial L2TP control packet out to establish a tunnel.
l2tp tunnel retransmit timeout	Configures the amount of time that the router waits before resending an L2TP control packet.
l2tp tunnel timeout no-session	Sets the duration a router waits after an L2TP tunnel becomes empty before tearing down the tunnel.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.
vpdn-template	Creates a VPDN template and enters VPDN template configuration mode.

l2tp tunnel retransmit timeout

To configure the amount of time that the router waits before resending a Layer 2 Tunneling Protocol (L2TP) control packet, use the **l2tp tunnel retransmit timeout** command in VPDN group configuration or VPDN template configuration mode. To disable a parameter setting, use the **no** form of this command.

l2tp tunnel retransmit timeout {**min** | **max**} *seconds*

no l2tp tunnel retransmit timeout {**min** | **max**} *seconds*

Syntax Description

min	Specifies the minimum time that the router waits before resending a control packet.
max	Specifies the maximum time that the router waits before resending a control packet.
seconds	Timeout length, in seconds, that the router waits before resending a control packet. The range is 1 to 8. The default minimum value is 1. The default maximum value is 8.

Command Default

The router uses the default timeout values: 1 second minimum and 8 seconds maximum.

Command Modes

VPDN group configuration (config-vpdn)

VPDN template configuration (config-vpdn-temp)

Command History

Release	Modification
12.0(7)DC	This command was introduced on the Cisco 6400 node route processor (NRP).
12.1(1)	This command was integrated into Cisco IOS Release 12.1(1).
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

Control channel retransmissions follow an exponential backoff, starting at the minimum retransmit timeout length specified by the **min** *seconds* keyword and argument. After each packet that is not acknowledged, the timeout exponentially increases until it reaches the value specified by the **max** *seconds* keyword and argument. For example, if the minimum timeout length is set to 1 second, the next retransmission attempt occurs 2 seconds later. The following attempt occurs 4 seconds later, and all additional attempts occur in 8-second intervals.

Cisco 10000 Series Router

We recommend that you configure the L2TP tunnel retransmit timeout to 2 seconds (minimum) and 8 seconds (maximum) on the Cisco 10000 series router.

Examples

The following example configures the VPDN group named group1 to make 8 retransmission attempts, with the minimum timeout length set at 2 seconds, and the maximum timeout length set at 4 seconds:

```
vpdn-group group1
 l2tp tunnel retransmit retries 8
 l2tp tunnel retransmit timeout min 2
 l2tp tunnel retransmit timeout max 4
```

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	Configures the number of times that the router attempts to send the initial L2TP control packet for tunnel establishment before considering a peer busy.
l2tp tunnel retransmit initial timeout	Configures the amount of time that the router waits before resending an initial L2TP control packet to establish a tunnel.
l2tp tunnel retransmit retries	Configures the number of retransmission attempts made for an L2TP control packet.
l2tp tunnel timeout no-session	Sets the duration a router waits after an L2TP tunnel becomes empty before tearing down the tunnel.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.
vpdn-template	Creates a VPDN template and enters VPDN template configuration mode.

l2tp tunnel timeout no-session

To configure the time a router waits after a Layer 2 Tunneling Protocol (L2TP) tunnel becomes empty before tearing down the tunnel, use the **l2tp tunnel timeout no-session** command in VPDN group or VPDN template configuration mode. To restore the default timeout value, use the **no** form of this command.

l2tp tunnel timeout no-session {*seconds* | **never**}

no l2tp tunnel timeout no-session

Syntax Description

seconds	Time, in seconds, the router waits before tearing down an empty L2TP tunnel. The range is 0 to 86400. If the router is configured as a network access server (NAS), the default is 15 seconds. If the router is configured as a tunnel server, the default is 10 seconds.
never	Specifies that the router never tears down an empty L2TP tunnel.

Command Default

Empty tunnels are torn down after the default timeout.

Command Modes

VPDN group configuration (config-vpdn)

VPDN template configuration (config-vpdn-temp)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(11)T	Support was added for the **never** keyword.

Usage Guidelines

Use the **l2tp tunnel timeout no-session** command to configure the amount of time a device waits before tearing down an empty tunnel. It might be desirable to leave an empty tunnel up beyond the default timeout value if you expect that a new session will be established imminently, or if you want to display statistics for a tunnel after all sessions have been terminated.

A router is considered a NAS if it has either a request-dialin or accept-dialout virtual private dialup network (VPDN) group configured.

A router is considered a tunnel server if it has either an accept-dialin or request-dialout VPDN group configured.

Examples

The following example configures the router to never tear down empty L2TP tunnels associated with the VPDN group named group1:

```
vpdn-group group1
 l2tp tunnel timeout no-session never
```

The following example returns the router to the default timeout duration for tearing down empty L2TP tunnels. This default value depends on whether the router is configured as a NAS or a tunnel server.

```
vpdn-group group1
 no l2tp tunnel timeout no-session
```

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 dial-in 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 dial-out 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 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
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.
vpdn-template	Creates a VPDN template and enters VPDN template configuration mode.

l2tp tunnel timeout setup

To configure the amount of time that the router waits for a confirmation message after sending the initial Layer 2 Tunneling Protocol (L2TP) control packet before considering a peer busy, use the **l2tp tunnel timeout setup** command in VPDN group or VPDN template configuration mode. To restore the default value, use the **no** form of this command.

l2tp tunnel timeout setup *seconds*

no l2tp tunnel timeout setup *seconds*

Syntax Description

seconds	Time, in seconds, the router waits for a return message. The range is 60 to 6000 seconds. The default is 10 seconds.

Command Default

The router waits 10 seconds for a confirmation message from the peer device before considering it busy.

Command Modes

VPDN group configuration (config-vpdn)

VPDN template configuration (config-vpdn-temp)

Command History

Release	Modification
12.1(1)	This command was introduced.

Usage Guidelines

If the router does not receive a confirmation message from the peer device before the tunnel timeout setup timer expires, the router places the peer on the busy list.

Examples

The following example configures a router to wait 25 seconds for confirmation that the initial L2TP control packet was received by the peer. This configuration applies only to tunnels associated with the virtual private dialup network (VPDN) group named group1.

```
vpdn-group group1
 l2tp tunnel timeout setup 25
```

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.

l2tp tunnel zlb delay

To configure the delay time before a zero length bit (ZLB) control message must be acknowledged, use the **l2tp tunnel zlb delay** command in VPDN group or VPDN template configuration mode. To restore the default value, use the **no** form of this command.

l2tp tunnel zlb delay *seconds*

no l2tp tunnel zlb delay *seconds*

Syntax Description

seconds	Maximum number of seconds the router delays before acknowledging ZLB control messages. The range is 1 to 5. The default is 3.

Command Default

The router waits up to 3 seconds before acknowledging ZLB control messages.

Command Modes

VPDN group configuration (config-vpdn)

VPDN template configuration (config-vpdn-temp)

Command History

Release	Modification
12.2(10)	This command was introduced.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

Use the**l2tp tunnel zlb delay** command to change the maximum allowable delay in responding to ZLB messages in a virtual private dialup network (VPDN) deployment. Changing the delay time can be beneficial when the peer device at the other end of the control channel requires a faster response to ZLB messages. This situation can occur if the remote peer has short keepalive timers configured.

Examples

The following example configures control channels associated with the VPDN group named group1 to delay no more than 2 seconds before responding to a ZLB message:

```
vpdn-group group1
 l2tp tunnel zlb delay 2
```

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.

l2tp tx-speed

To configure the transmit-speed (tx-speed) value for Layer 2 Tunneling Protocol (L2TP) to be sent to the L2TP network server (LNS), use the **l2tp tx-speed** command in VPDN group configuration or VPDN template configuration mode. To return to the default value, use the **no** form of this command.

l2tp tx-speed {*value* | **ancp** [*value*] | **ram-min** [*value*]}

no l2tp tx-speed {*value* | **ancp** [*value*] | **ram-min** [*value*]}

Syntax Description

ancp	Specifies that the source to obtain the tx-speed value is Access Node Control Protocol (ANCP).
ram-min	Specifies that the source to obtain the tx-speed value is Rate Adaptive Mode-minimum (RAM-min).
value	(Optional) The tx-speed value in kilobits per second (kbps). The range is 0 to 2147483.

Command Default

L2TP obtains the tx-speed value from Point-to-Point Protocol over Ethernet (PPPoE) and sends it to the LNS.

Command Modes

VPDN group configuration (config-vpdn)

VPDN template configuration (config-vpdn-temp)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines

Use the **l2tp tx-speed** command to configure the tx-speed value that the L2TP sends to the LNS.

- If the source specified is ANCP, L2TP sends the downstream value configured for ANCP to the LNS.
- If the source specified is RAM-min, L2TP sends the tx-speed value configured for RAM-min to the LNS.
- If the tx-speed is not configured for ANCP or RAM-min, L2TP sends the tx-speed value specified in the command.

Examples

The following example shows how to configure the tx-speed value locally:

```
Router(config)# vpdn-group 1
Router(config-vpdn)# l2tp tx-speed 8000
```

The following example shows how to configure the tx-speed value obtained from ANCP, and if the tx-speed is not configured for ANCP, L2TP sends the locally configured tx-speed value to the LNS:

```
Router(config)# vpdn-template 2
Router(config-vpdn-temp)# l2tp tx-speed ancp 15000
```

The following example shows how to configure the tx-speed value obtained from RAM-min, and if the tx-speed is not configured for RAM-min, L2TP sends the locally configured tx-speed value to the LNS.

```
Router(config)# vpdn-group 1
Router(config-vpdn)# l2tp tx-speed ram-min 10000
```

Related Commands

Command	Description
l2tp rx-speed	Configures the rx-speed value to be sent to the LNS.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.
vpdn-template	Creates a VPDN template and enters VPDN template configuration mode.

lcp renegotiation

To allow the L2TP network server (LNS) to renegotiate the PPP Link Control Protocol (LCP) on dial-in calls, using Layer 2 Tunneling Protocol (L2TP) or Layer 2 Forwarding (L2F), use the **lcp renegotiation** command in virtual private dialup network (VPDN) group configuration mode. To remove LCP renegotiation, use the **no** form of this command.

lcp renegotiation {**always** | **on-mismatch**}

no lcp renegotiation

Syntax Description

always	Always renegotiate LCP at the LNS.
on-mismatch	Renegotiate LCP at the LNS only in the event of an LCP mismatch between the LAC and the LNS.

Command Default

LCP renegotiation is disabled on 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 subgroup is enabled.

Usage Guidelines

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

This command is valid only at the LNS. This command is useful for an LNS that tunnels to a non-Cisco L2TP access concentrator (LAC), where the LAC might negotiate a different set of LCP options than what the LNS expects.

When a PPP session is started at the LAC, LCP parameters are negotiated, and a tunnel is initiated, the LNS can either accept the LAC LCP negotiations or can request LCP renegotiation. Using the **lcp renegotiation always** command forces renegotiation to occur at the LNS. If the **lcp renegotiation on-**

mismatch command is configured, then renegotiation occurs only if there is an LCP mismatch between the LNS and LAC.

Note Older PC PPP clients might experience a *lock up* during PPP LCP renegotiation.

Examples

The following example configures the LNS to renegotiate PPP LCP with a non-Cisco LAC:

```
vpdn-group 1
 accept dialin
  protocol l2tp
  virtual-template 1
 terminate-from router32
 lcp renegotiation on-mismatch
```

Related Commands

Command	Description
accept-dialin	Specifies the LNS to use for authenticating--and the virtual template to use for cloning--new virtual access interfaces when an incoming L2TP tunnel connection is requested from a specific peer.
force-local-chap	Forces the LNS to reauthenticate the client.

loadsharing

To configure endpoints for load sharing, use the **loadsharing** command in virtual private dialup network (VPDN) group configuration mode. To remove this function, use the **no** form of this command.

loadsharing ip *ip-address* [**limit** *session-limit*]

no loadsharing ip *ip-address* [**limit** *session-limit*]

Syntax Description

ip *ip-address*	IP address of the home gateway/L2TP network server (HGW/LNS) at the other end of the tunnel. This is the IP endpoint at the end of the tunnel, which is a HGW/LNS router.
limit *session-limit*	(Optional) Limits sessions per load share. The range is 0 to 32,767 sessions. By default, no limit is set.

Command Default

No default is set, and this function is not used when not configured.

Command Modes

VPDN group configuration (config-vpdn)

Command History

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

Usage Guidelines

Use the **loadsharing** VPDN group configuration command to configure endpoints for loadsharing.

Examples

In the following example, VPDN group customer1-vpdng is created. L2TP IP traffic load is shared between two HGW/LNS. The IP addresses for the HGW/LNS WAN ports are 172.21.9.67 and 172.21.9.68 (the home gateway is a Cisco IOS router terminating L2TP sessions). The characteristics for link 172.21.9.67 are defined by using the **request dialin** command. The characteristics for link 172.21.9.68 are defined by using the **loadsharing** command.

A backup home-gateway router is specified at 172.21.9.69 by using the **backup** command. This router serves as a backup device for two load-sharing HGW/LNS:

```
vpdn-group customer1-vpdng
 request dialin l2tp ip 172.21.9.67 domain cisco.com
 loadsharing ip 172.21.9.68 limit 100
```

```
backup ip 172.21.9.69 priority 5
domain cisco2.com
```

Related Commands

Command	Description
request-dialin	Configures an L2TP access concentrator 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.

local name

To specify a local hostname that the tunnel uses to identify itself, use the **local name** command in VPDN group or VPDN template configuration mode. To remove the configured local hostname, use the **no** form of this command.

local name *host-name*

no local name

Syntax Description

host-name	Local hostname of the tunnel.

Command Default

No local hostname is configured.

Command Modes

VPDN group configuration (config-vpdn)

VPDN template configuration (config-vpdn-temp)

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.

Usage Guidelines

This command allows each virtual private dialup network (VPDN) group to use a unique local hostname. The password hierarchy sequence that is used for tunnel identification and, subsequently, tunnel authentication, is as follows:

- A Layer 2 Tunneling Protocol (L2TP) tunnel password is used first (defined by the **l2tp tunnel password** command).
- If no L2TP tunnel password exists, the password associated with the local name is used.
- If no local name password exists, the password associated with the hostname is used.

The **username** command defines the passwords associated with the local name and the hostname.

Examples

The following example configures the local hostname Tunnel1 for the tunnels associated with the VPDN group named tunnelme:

```
vpdn-group tunnelme
 local name Tunnel1
```

Related Commands

Command	Description
l2tp tunnel password	Sets the password the router uses to authenticate the tunnel.
username	Establishes a username-based authentication system.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.
vpdn-template	Creates a VPDN template and enters VPDN template configuration mode.

M through T

multihop-hostname

To enable a tunnel switch to initiate a tunnel based on the hostname or tunnel ID associated with an ingress tunnel, use the **multihop-hostname** command in VPDN request-dialin subgroup configuration mode. To disable this option, use the **no** form of this command.

multihop-hostname *ingress-tunnel-name*

no multihop-hostname *ingress-tunnel-name*

Syntax Description

ingress-tunnel-name	Network access server (NAS) hostname or ingress tunnel ID.

Command Default

No multihop hostname is configured.

Command Modes

VPDN request-dialin subgroup configuration (config-vpdn-req-in)

Command History

Release	Modification
12.1(1)DC1	This command was introduced on the Cisco 6400 node route processor (NRP).
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 **multihop-hostname** command only on a device configured as a tunnel switch.

The *ingress-tunnel-name* argument must specify either the hostname of the device initiating the tunnel that is to be to be switched, or the tunnel ID of the ingress tunnel that is to be switched.

Removing the request-dialin subgroup configuration removes the **multihop-hostname** configuration.

Examples

The following example configures a Layer 2 Tunneling Protocol (L2TP) virtual private dialup network (VPDN) group on a tunnel switch to forward ingress sessions from the host named LAC-1 through an outgoing tunnel to IP address 10.3.3.3:

```
vpdn-group 11
 request-dialin
```

```
protocol l2tp
multihop-hostname LAC-1
initiate-to ip 10.3.3.3
local name tunnel-switch
```

Related Commands

Command	Description
dnis	Configures a VPDN group to tunnel calls from the specified DNIS, and supports additional domain names for a specific VPDN group.
domain	Requests that PPP calls from a specific domain name be tunneled, and supports additional domain names for a specific VPDN group.
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.
vpdn multihop	Enables VPDN multihop.
vpdn search-order	Specifies how the NAS is to perform VPDN tunnel authorization searches.

pool-member

To assign a request-dialout virtual private dialup network (VPDN) subgroup to a dialer pool, use the **pool-member** command in VPDN request-dialout configuration mode. To remove the request-dialout VPDN subgroup from a dialer pool, use the **no** form of this command.

pool-member *pool-number*

no pool-member [*pool-number*]

Syntax Description

pool-number	Dialer pool to which this VPDN group belongs.

Command Default

Command is disabled.

Command Modes

VPDN request-dialout configuration (config-vpdn-req-ou)

Command History

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

Usage Guidelines

Before you can enable the **pool-member** command, you must first enable the **protocol l2tp** command on the request-dialout VPDN subgroup. Removing the **protocol l2tp** command removes the **pool-member** command from the request-dialout VPDN subgroup.

You can configure only one dialer profile pool (by using the **pool-member** command) or dialer rotary group (by using the **rotary-group** command). If you attempt to configure a second dialer resource, you replace the first dialer resource in the configuration.

Examples

The following example configures VPDN group 1 to request L2TP dial-out to IP address 172.16.4.6 using dialer profile pool 1 and identifying itself using the local name *user1*.

```
vpdn-group 1
 request-dialout
  protocol l2tp
  pool-member 1
 initiate-to ip 172.16.4.6
 local name user1
```

Related Commands

Command	Description
initiate-to	Specifies the IP address that will be tunneled to.
protocol (VPDN)	Specifies the Layer 2 tunneling protocol that the VPDN subgroup will use.
request-dialout	Enables an LNS to request VPDN dial-out calls by using L2TP.
rotary-group	Assigns a request-dialout VPDN subgroup to a dialer rotary group.

pptp flow-control receive-window

To specify how many packets the Point-to-Point Tunnel Protocol (PPTP) client can send before it must wait for acknowledgment from the tunnel server, use the **pptp flow-control receive-window** command in VPDN group or VPDN template configuration mode. To restore the default value, use the **no** form of this command.

pptp flow-control receive-window *packets*

no pptp flow-control receive-window

Syntax Description

packets	Number of packets the client can send before it waits for acknowledgment from the tunnel server. The range is 1 to 64 packets. The default is 16 packets.

Command Default

The PPTP client can send up to 16 packets before it must wait for acknowledgment.

Command Modes

VPDN group configuration (config-vpdn)

VPDN template configuration (config-vpdn-temp)

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.

Examples

The following example shows how to fine-tune PPTP by specifying that a client associated with the virtual private dialup network (VPDN) group named group1 can send 20 packets before it must wait for acknowledgment from the tunnel server:

```
vpdn-group group1
 accept-dialin
  protocol pptp
  virtual-template 1
!
 pptp flow-control receive-window 20
```

Related Commands

Command	Description
encryption mppe	Enables MPPE encryption on the virtual template.
pptp flow-control static-rtt	Specifies the tunnel server’s timeout interval between sending a packet to the client and receiving a response.
pptp tunnel echo	Specifies the period of idle time on the tunnel that triggers an echo message from the tunnel server to the client.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.
vpdn-template	Creates a VPDN template and enters VPDN template configuration mode.

pptp flow-control static-rtt

To specify the timeout interval of the Point-to-Point Tunnel Protocol (PPTP) tunnel server between sending a packet to the client and receiving a response, use the **pptp flow-control static-rtt** command in VPDN group or VPDN template configuration mode. To restore the default value, use the **no** form of this command.

pptp flow-control static-rtt *seconds*

no pptp flow-control static-rtt

Syntax Description

seconds	Timeout interval, in milliseconds (ms), that the tunnel server waits between sending a packet to the client and receiving a response. The range is 100 to 5000. The default is 1500.

Command Default

The tunnel server waits 1500 ms for a response before timing out.

Command Modes

VPDN group configuration (config-vpdn)

VPDN template configuration (config-vpdn-temp)

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

If the session times out, the tunnel server does not retry or resend the packet. Instead the flow control alarm is set off, and stateful mode is automatically switched to stateless.

Examples

The following example shows how to fine-tune PPTP by increasing the timeout interval for tunnels associated with the virtual private dialup network (VPDN) group named group1 on the tunnel server to 2000 ms:

```
vpdn-group group1
 accept-dialin
  protocol pptp
  virtual-template 1
```

```
!
 pptp flow-control static-rtt 2000
```

Related Commands

Command	Description
encryption mppe	Enables MPPE encryption on the virtual template.
pptp flow-control receive-window	Specifies how many packets the client can send before it must wait for the acknowledgment from the tunnel server.
pptp tunnel echo	Specifies the period of idle time on the tunnel that triggers an echo message from the tunnel server to the client.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.
vpdn-template	Creates a VPDN template and enters VPDN template configuration mode.

pptp tunnel echo

To specify the period of idle time on the Point-to-Point Tunnel Protocol (PPTP) tunnel that triggers an echo message from the tunnel server to the client, use the **pptp tunnel echo** command in VPDN group or VPDN template configuration mode. To restore the default value, use the **no** form of this command.

pptp tunnel echo *seconds*

no pptp tunnel echo

Syntax Description

seconds	Echo packet interval, in seconds. The range is 0 to 1000. The default is 60.

Command Default

The tunnel server sends an echo message after a 60-second idle interval.

Command Modes

VPDN group configuration (config-vpdn)

VPDN template configuration (config-vpdn-temp)

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

Use the **pptp tunnel echo** command to set the idle time that the tunnel server waits before sending an echo message to the client.

If the tunnel server does not receive a reply to the echo message within 20 seconds, it tears down the tunnel. This 20-second interval is hard coded.

Examples

The following example shows how to fine-tune PPTP on the tunnel server by increasing the idle time interval for the tunnels associated with the virtual private dialup network (VPDN) group named group1 to 90 seconds:

```
vpdn-group group1
 accept-dialin
  protocol pptp
  virtual-template 1
```

```
!
 pptp tunnel echo 90
```

Related Commands

Command	Description
encryption mppe	Enables MPPE encryption on the virtual template.
pptp flow-control receive-window	Specifies how many packets the client can send before it must wait for the acknowledgment from the tunnel server.
pptp flow-control static-rtt	Specifies the timeout interval of the tunnel server between sending a packet to the client and receiving a response.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.
vpdn-template	Creates a VPDN template and enters VPDN template configuration mode.

protocol (VPDN)

To specify the tunneling protocol that a virtual private dialup network (VPDN) subgroup uses, use the **protocol** command in the appropriate VPDN subgroup configuration mode. To remove the protocol-specific configurations from a VPDN subgroup, use the **no** form of this command.

protocol {**any** | **l2f** | **l2tp** | **pppoe** | **pptp**}

no protocol {**any** | **l2f** | **l2tp** | **pppoe** | **pptp**}

Syntax Description

any	Specifies either the Layer 2 Forwarding (L2F) protocol or the Layer 2 Tunneling Protocol (L2TP).
l2f	Specifies the L2F protocol. **Note** The **l2f** keyword was removed from Cisco IOS Release 12.4(11)T.
l2tp	Specifies L2TP.
pppoe	Specifies the PPP over Ethernet (PPPoE) protocol.
pptp	Specifies the Point-to-Point Tunneling Protocol (PPTP).

Command Default

No protocol is specified.

Command Modes

VPDN accept-dialin group configuration (config-vpdn-acc-in)

VPDN accept-dialout group configuration (config-vpdn-acc-out)

VPDN request-dialin group configuration (config-vpdn-acc-in)

VPDN request-dialout group configuration (config-vpdn-req-out)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.1(1)T	The **pppoe** keyword was added.
12.4(11)T	The **l2f** keyword was removed from Cisco IOS Release 12.4(11)T.

Release	Modification
Cisco IOS XE Release 2.5.0	This command was implemented on Cisco ASR 1000 series routers.

Usage Guidelines

This command is required for any VPDN subgroup configuration.

L2TP is the only protocol that can be used for dialout subgroup configurations.

Removal of l2f Keyword

The **l2f** keyword was removed from Cisco IOS Release 12.4(11)T. It is available in releases prior to Release 12.4(11)T.

Changing the protocol removes all the commands from the VPDN subgroup configuration, and any protocol-specific commands from the VPDN group configuration.

Note Users must first enter the **vpdn enable** command to configure the PPP over Ethernet discovery daemon.

The **show running-config** command does not display the configured domain name and virtual template unless you configure the **protocol l2tp** command.

When you unconfigure the **protocol l2tp** command, the configured domain name and virtual template are automatically removed. When you reconfigure the **protocol l2tp** command, the domain name and virtual template need to be explicitly added again.

Examples

The following example configures VPDN group 1 to accept dial-in calls using L2F and to request dial-out calls using L2TP:

```
Router> enable
Router# configure terminal
Router(config)# vpdn enable
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-acc-in)# exit

Router(config-vpdn)# request-dialout
Router(config-vpdn-req-out)# protocol l2tp
Router(config-vpdn-req-out)# pool-member 1
Router(config-vpdn-acc-in)# exit
Router(config-vpdn)# local name router1
Router(config-vpdn)# terminate-from hostname router2
Router(config-vpdn)# initiate-to ip 10.3.2.1
Router(config-vpdn)# l2f ignore-mid-sequence
Router(config-vpdn)# l2tp ip udp checksum
```

If you then use the **no protocol** command in VPDN request-dialout group configuration mode, the configuration changes to this:

```
vpdn enable
!
vpdn-group 1
 accept-dialin
  protocol l2f
  virtual-template 1
 terminate-from hostname router2
 local name router1
 l2f ignore-mid-sequence
The following example shows how to set VPDN group 1 to request dial-in calls using PPTP:
Router> enable
Router# configure terminal
Router(config)# vpdn enable
Router(config)# vpdn-group 1
Router(config-vpdn)# request-dialin

Router(config-vpdn-req-in)# protocol pptp
```

The **domain** *name* command configures the domain name of the users that will be forwarded to the L2TP tunnel server. The **virtual-template** command selects the default virtual template from which to clone the virtual access interfaces for the L2TP tunnel. The following example shows how to configure the **protocol l2tp**, **virtual-template**, and the **domain** *name* commands:

```
Router(config)# vpdn enable
Router(config)# vpdn-group l2tp
Router(config-vpdn)# request-dialin
Router(config-vpdn-req-in)# protocol l2tp
Router(config-vpdn-req-in)# virtual-template 1
Router(config-vpdn-req-in)# domain example.com
Router(config-vpdn-req-in)# exit
```

If you then use the **no protocol** command in VPDN request-dialout group configuration mode, the configuration changes to this:

```
vpdn enable
!
vpdn-group l2tp
```

The following example shows the output from the **show running-config** command, if you reconfigure the **protocol l2tp** command:

```
vpdn enable
!
vpdn-group l2tp
 request-dialin
  protocol l2tp
```

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 VPDN accept-dialin group 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 VPDN accept-dialout group 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 VPDN request-dialin group configuration mode.

Command	Description
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 VPDN request-dialout group configuration mode.
vpdn enable	Enables VPDN on the router and informs the router to look for tunnel definitions in a local database and on a remote authorization server (home gateway).
vpdn-group	Associates a VPDN group with a customer or VPDN profile.

radius-server attribute 31 remote-id

To override the calling-station-id attribute with remote-id in RADIUS AAA messages, use the **radius-server attribute 31 remote-id** command in global configuration mode. To disable the command function (default), use the **no** form of this command.

radius-server attribute 31 remote-id

no radius-server attribute 31 remote-id

Syntax Description

This command has no arguments or keywords.

Command Default

Command function is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(6th)T	This command was introduced.

Usage Guidelines

Configure the **radius-server attribute 31 remote-id** command on the L2TP network server (LNS).

Examples

The following example shows the configuration on the LNS:

```
LNS(config)# radius-server attribute 31 remote-id
```

Related Commands

Command	Description
debug vpdn	Displays information associated with the RADIUS server.
dsl-line-info-forwarding	Enables the transfer of VSAs from the LAC to the LNS.
radius-server attribute 87 circuit-id	Overrides the nas-port-id attribute with circuit-id in RADIUS AAA messages.

Command	Description
vpdn-group	Creates a virtual private dialup network (VPDN) group and enters VPDN group configuration mode.

radius-server attribute 87 circuit-id

To override the nas-port-id attribute with Circuit_ID in RADIUS AAA messages, use the **radius-server attribute 87 circuit-id** command in global configuration mode. To disable the command function (default), use the **no** form of this command.

radius-server attribute 87 circuit-id

no radius-server attribute 87 circuit-id

Syntax Description

This command has no arguments or keywords.

Command Default

The command function is disabled.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

Configure the **radius-server attribute 87 circuit-id** command on the L2TP network server (LNS).

Examples

The following example shows the configuration on the LNS:

```
LNS(config)# radius-server attribute 87 circuit-id
```

Related Commands

Command	Description
debug vpdn	Displays information associated with the RADIUS server.
dsl-line-info-forwarding	Enables the transfer of VSAs from the LAC to the LNS.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.

radius-server domain-stripping

To configure a network access server (NAS) to strip suffixes, or to strip both suffixes and prefixes from the username before forwarding the username to the remote RADIUS server, use the **radius-server domain-stripping** command in global configuration mode. To disable a stripping configuration, use the **no** form of this command.

Note The **ip vrf default** command must be configured in global configuration mode before the **radius-server domain-stripping** command is configured to ensure that the default VRF name is a NULL value until the default vrf name is configured.

```
radius-server domain-stripping [[right-to-left] [prefix-delimiter character [character2 ...
character7]] [delimiter character [character2 ... character7]] | strip-suffix suffix] [vrf vrf-name]

no radius-server domain-stripping [[right-to-left] [prefix-delimiter character [character2 ...
character7]] [delimiter character [character2 ... character7]] | strip-suffix suffix] [vrf vrf-name]
```

Syntax Description

right-to-left	(Optional) Specifies that the NAS applies the stripping configuration at the first delimiter found when parsing the full username from right to left. The default is for the NAS to apply the stripping configuration at the first delimiter found when parsing the full username from left to right.
prefix-delimiter *character* [*character2...character7*]	(Optional) Enables prefix stripping and specifies the character or characters that are recognized as a prefix delimiter. Valid values for the *character* argument are @, /, $, %, \, #, and -. Multiple characters can be entered without intervening spaces. Up to seven characters can be defined as prefix delimiters, which is the maximum number of valid characters. If a \ is entered as the final or only value for the *character* argument, it must be entered as \\. No prefix delimiter is defined by default.
delimiter *character* [*character2...character7*]	(Optional) Specifies the character or characters that are recognized as a suffix delimiter. Valid values for the *character* argument are @, /, $, %, \, #, and -. Multiple characters can be entered without intervening spaces. Up to seven characters can be defined as suffix delimiters, which is the maximum number of valid characters. If a \ is entered as the final or only value for the *character* argument, it must be entered as \\. The default suffix delimiter is the @ character.

strip-suffix *suffix*	(Optional) Specifies a suffix to strip from the username.
vrf *vrf-name*	(Optional) Restricts the domain stripping configuration to a Virtual Private Network (VPN) routing and forwarding (VRF) instance. The *vrf-name* argument specifies the name of a VRF.

Command Default

Stripping is disabled. The full username is sent to the RADIUS server.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(2)DD	This command was introduced on the Cisco 7200 series and Cisco 7401ASR.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3(4)T	Support was added for the **right-to-left** and the **delimiter** *character* keywords and argument.
12.4(4)T	Support was added for the **strip-suffix** *suffix* and the **prefix-delimiter** keywords and argument.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.(33)SRC.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
XE 2.1	This command was integrated into Cisco IOS Release XE 2.1.
XE 2.5	Support was added for the **strip-suffix** *suffix* and the **prefix-delimiter** keywords and argument.

Usage Guidelines

Use the **radius-server domain-stripping** command to configure the NAS to strip the domain from a username before forwarding the username to the RADIUS server. If the full username is user1@cisco.com, enabling the **radius-server domain-stripping** command results in the username *user1* being forwarded to the RADIUS server.

Use the **right-to-left** keyword to specify that the username should be parsed for a delimiter from right to left, rather than from left to right. This allows strings with two instances of a delimiter to strip the username at either delimiter. For example, if the username is user@cisco.com@cisco.net, the suffix could be stripped in two ways. The default direction (left to right) results in the username *user* being forwarded to the RADIUS server. Configuring the **right-to-left** keyword results in the username *user@cisco.com* being forwarded to the RADIUS server.

Use the **prefix-delimiter** keyword to enable prefix stripping and to specify the character or characters that are recognized as a prefix delimiter. The first configured character that is parsed is used as the prefix delimiter, and any characters before that delimiter are stripped.

Use the **delimiter** keyword to specify the character or characters that are recognized as a suffix delimiter. The first configured character that is parsed is used as the suffix delimiter, and any characters after that delimiter are stripped.

Use the **strip-suffix** *suffix* option to specify a particular suffix to strip from usernames. For example, configuring the **radius-server domain-stripping strip-suffix cisco.net** command results in the username user@cisco.net being stripped, while the username user@cisco.com is not stripped. You can configure multiple suffixes for stripping by issuing multiple instances of the **radius-server domain-stripping** command. The default suffix delimiter is the @ character.

Note Issuing the **radius-server domain-stripping strip-suffix** *suffix* command disables the capacity to strip suffixes from all domains. Both the suffix delimiter and the suffix must match for the suffix to be stripped from the full username. The default suffix delimiter of @ will be used if you do not specify a different suffix delimiter or set of suffix delimiters using the **delimiter** keyword.

To apply a domain-stripping configuration only to a specified VRF, use the **vrf** *vrf-name* option.

The interactions between the different types of domain stripping configurations are as follows:

- You can configure only one instance of the **radius-server domain-stripping** [**right-to-left**] [**prefix-delimiter** *character* [*character2...character7*]] [**delimiter** *character* [*character2...character7*]] command.
- You can configure multiple instances of the **radius-server domain-stripping** [**right-to-left**] [**prefix-delimiter** *character* [*character2...character7*]] [**delimiter** *character* [*character2...character7*]] [**vrf** *vrf-name*] command with unique values for **vrf** *vrf-name*.
- You can configure multiple instances of the **radius-server domain-stripping strip-suffix** *suffix* [**vrf** *per-vrf*] command to specify multiple suffixes to be stripped as part of a global or per-VRF ruleset.
- Issuing any version of the **radius-server domain-stripping** command automatically enables suffix stripping using the default delimiter character @ for that ruleset, unless a different delimiter or set of delimiters is specified.
- Configuring a per-suffix stripping rule disables generic suffix stripping for that ruleset. Only suffixes that match the configured suffix or suffixes will be stripped from usernames.

Examples

The following example configures the router to parse the username from right to left and sets the valid suffix delimiter characters as @, \, and $. If the full username is cisco/user@cisco.com$cisco.net, the username “cisco/user@cisco.com” will be forwarded to the RADIUS server because the $ character is the first valid delimiter encountered by the NAS when parsing the username from right to left.

```
radius-server domain-stripping right-to-left delimiter @\$
```

The following example configures the router to strip the domain name from usernames only for users associated with the VRF instance named abc. The default suffix delimiter @ is used for generic suffix stripping.

```
radius-server domain-stripping vrf abc
```

The following example enables prefix stripping using the character / as the prefix delimiter. The default suffix delimiter character @ is used for generic suffix stripping. If the full username is cisco/user@cisco.com, the username “user” is forwarded to the RADIUS server.

```
radius-server domain-stripping prefix-delimiter /
```

The following example enables prefix stripping, specifies the character / as the prefix delimiter, and specifies the character # as the suffix delimiter. If the full username is cisco/user@cisco.com#cisco.net, the username “user@cisco.com” is forwarded to the RADIUS server.

```
radius-server domain-stripping prefix-delimiter / delimiter #
```

The following example enables prefix stripping, configures the character / as the prefix delimiter, configures the characters $, @, and # as suffix delimiters, and configures per-suffix stripping of the suffix cisco.com. If the full username is cisco/user@cisco.com, the username “user” is forwarded to the RADIUS server. If the full username is cisco/user@cisco.com#cisco.com, the username “user@cisco.com” is forwarded.

```
radius-server domain-stripping prefix-delimiter / delimiter $@#
radius-server domain-stripping strip-suffix cisco.com
```

The following example configures the router to parse the username from right to left and enables suffix stripping for usernames with the suffix cisco.com. If the full username is cisco/user@cisco.net@cisco.com, the username “cisco/user@cisco.net” is forwarded to the RADIUS server. If the full username is cisco/user@cisco.com@cisco.net, the full username is forwarded.

```
radius-server domain-stripping right-to-left
radius-server domain-stripping strip-suffix cisco.com
```

The following example configures a set of global stripping rules that strip the suffix cisco.com using the delimiter @, and a different set of stripping rules for usernames associated with the VRF named myvrf:

```
radius-server domain-stripping strip-suffix cisco.com
!
radius-server domain-stripping prefix-delimiter # vrf myvrf
radius-server domain-stripping strip-suffix cisco.net vrf myvrf
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.
ip vrf	Defines a VRF instance and enters VRF configuration mode.

Command	Description
tacacs-server domain-stripping	Configures a router to strip a prefix or suffix from the username before forwarding the username to the TACACS+ server.

redirect identifier

To configure a virtual private dialup network (VPDN) redirect identifier to use for Layer 2 Tunneling Protocol (L2TP) call redirection on a network access server (NAS), use the **redirect identifier** command in VPDN group or VPDN template configuration mode. To remove the name of the redirect identifier from the NAS, use the **no** form of this command.

redirect identifier *identifier-name*

no redirect identifier *identifier-name*

Syntax Description

identifier-name	Name of the redirect identifier to use for call redirection.

Command Default

No redirect identifier is configured.

Command Modes

VPDN group configuration (config-vpdn)

VPDN template configuration (config-vpdn-temp)

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.

Usage Guidelines

The **redirect identifier** command is used only on the NAS. To configure the name of the redirect identifier on the stack group tunnel server, use the **vpdn redirect identifier** command in global configuration mode.

The NAS compares the redirect identifier with the one received from the stack group tunnel server to determine authorization information to redirect the call.

Configuring the redirect identifier is not necessary to perform redirects. If the redirect identifier is not configured, the NAS uses the redirect IP address to obtain authorization information to redirect the call. In that case, the IP address of the new redirected tunnel server must be present in the **initiate-to** command configuration of the VPDN group on the NAS.

The redirect identifier allows new stack group members to be added without the need to update the NAS configuration with their IP addresses. With the redirect identifier configured, a new stack group member can be added and given the same redirect identifier as the rest of the stack group.

If the authorization information for getting to the new redirected tunnel server is different, then you must configure the authorization information via RADIUS using tagged attributes:

```
Cisco:Cisco-Avpair = :0:"vpdn:vpdn-redirect-id=
identifier name
"
```

The NAS chooses the correct tagged parameters to obtain authorization information for the new redirected tunnel server by first trying to match the redirect identifier (if present) or else by matching the Tunnel-Server-Endpoint IP address.

Examples

The following example configures the redirect identifier named lns1 on the NAS for the VPDN group named group1:

```
vpdn-group group1
 redirect identifier lns1
```

Related Commands

Command	Description
clear vpdn redirect	Clears the L2TP redirect counters shown in the output from the **show vpdn redirect** command.
show vpdn redirect	Displays statistics for L2TP call 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 LAC.
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 LNS.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.
vpdn-template	Creates a VPDN template and enters VPDN template configuration mode.

request-dialin

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

request-dialin

no request-dialin

Syntax Description

This command has no arguments or keywords.

Command Default

No request dial-in VPDN subgroups are configured.

Command Modes

VPDN group configuration

Command History

Release	Modification
11.3(5)AA	This command was introduced.
12.0(5)T	This command was integrated into Cisco IOS Release 12.0(5)T.
12.0(5)T	The original keywords and arguments were removed and made into separate **request-dialin** subgroup commands.

Usage Guidelines

Use the **request-dialin** command on a NAS to configure a VPDN group to request the establishment of dial-in VPDN tunnels to a tunnel server.

For a VPDN group to request dial-in calls, you must also configure the following commands:

- The **initiate-to**command in VPDN group configuration mode
- The **protocol** command in request dial-in VPDN subgroup configuration mode
- At least one **dnis** or **domain** command in request dial-in VPDN subgroup configuration mode

The NAS can also be configured to accept requests for Layer 2 Tunnel Protocol (L2TP) dial-out VPDN tunnels from the tunnel server using the **accept-dialout** command. Dial-in and dial-out calls can use the same L2TP tunnel.

Examples

The following example requests an L2TP dial-in tunnel to a remote peer at IP address 172.17.33.125 for a user in the domain named cisco.com:

```
Router(config)# vpdn-group 1
Router(config-vpdn)# request-dialin
Router(config-vpdn-req-in)# protocol l2tp
Router(config-vpdn-req-in)# domain cisco.com
!
Router(config-vpdn)# initiate-to ip 172.17.33.125
```

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 dial-in 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 dial-out VPDN subgroup configuration mode.
authen before-forward	Specifies that VPDN send the entire structured username to the AAA server the first time the router contacts the AAA server.
dnis	Specifies the DNIS group name or DNIS number of users that are to be forwarded to a tunnel server using VPDN.
domain	Specifies the domain name of users that are to be forwarded to a tunnel server using VPDN.
initiate-to	Specifies the IP address that calls are tunneled to.
protocol (VPDN)	Specifies the tunneling protocol that a VPDN subgroup will use.

request-dialout

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

request-dialout

no request-dialout

Syntax Description

This command has no arguments or keywords.

Command Default

No request 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.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

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

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

- The **initiate-to** command in VPDN group configuration mode
- The **protocol l2tp** command in request dial-out VPDN subgroup configuration mode
- Either the **pool-member** command or the **rotary-group** command in request dial-out VPDN subgroup configuration mode, depending on the type of dialer resource to be used by the VPDN subgroup
- The **dialer vpdn** command in dialer interface configuration mode

If the dialer pool or dialer rotary group that the VPDN group is in contains physical interfaces, the physical interfaces are used before the VPDN group configuration.

The tunnel server can also be configured to accept requests to establish dial-in VPDN tunnels from a NAS using the **accept-dialin** command. Dial-in and dial-out calls can use the same L2TP tunnel.

Cisco 10000 Series Router

The Cisco 10000 series router does not support Large-Scale Dial-Out (LSDO). The **request-dialout** command is not implemented.

Examples

The following example configures VPDN group 1 to request an L2TP tunnel to the peer at IP address 10.3.2.1 for tunneling dial-out calls from dialer pool 1:

```
Router(config)# vpdn-group 1
Router(config-vpdn)# request-dialout
Router(config-vpdn-req-ou)# protocol l2tp
Router(config-vpdn-req-ou)# pool-member 1
Router(config-vpdn-req-ou)# exit
Router(config-vpdn)# initiate-to ip 10.3.2.1
Router(config-vpdn)# exit
Router(config)# interface Dialer2
Router(config-if)# ip address 172.16.2.3 255.255.128
Router(config-if)# encapsulation ppp
Router(config-if)# dialer remote-name dialer32
Router(config-if)# dialer string 5550100
Router(config-if)# dialer vpdn
Router(config-if)# dialer pool 1
Router(config-if)# dialer-group 1
Router(config-if)# ppp authentication chap
```

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 dial-in 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 dial-out VPDN subgroup configuration mode.
dialer vpdn	Enables a dialer profile or DDR dialer to use L2TP dial-out.
initiate-to	Specifies the IP address that will be tunneled to.
pool-member	Assigns a request-dialout VPDN subgroup to a dialer pool.
protocol (VPDN)	Specifies the tunneling protocol that a VPDN subgroup uses.
rotary-group	Assigns a request-dialout VPDN subgroup to a dialer rotary group.

resource-pool profile vpdn

To create a virtual private dialup network (VPDN) profile and to enter VPDN profile configuration mode, use the **resource-pool profile vpdn** command in global configuration mode. To disable this function, use the **no** form of this command.

resource-pool profile vpdn *name*

no resource-pool profile vpdn *name*

Syntax Description

name	VPDN profile name.

Command Default

No VPDN profiles are set up.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(4)XI	This command was introduced.
12.0(5)T	Support for this command was integerated into Cisco IOS Release 12.0(5)T.

Usage Guidelines

Use the **resource-pool profile vpdn** command to create a VPDN profile and enter VPDN profile configuration mode, or to enter VPDN profile configuration mode for a VPDN profile that already exists.

VPDN groups can be associated with a VPDN profile by using the **vpdn group** command in VPDN profile configuration mode. A VPDN profile counts VPDN sessions across all associated VPDN groups.

VPDN session limits for the VPDN groups associated with a VPDN profile can be configured in VPDN profile configuration mode by using the **limit base-size** command.

Examples

The following example creates the VPDN groups named l2tp and l2f, and associates both VPDN groups with the VPDN profile named profile32:

```
Router(config)# vpdn-group l2tp
Router(config-vpdn)#
!
Router(config)# vpdn-group l2f
Router(config-vpdn)#
!
Router(config)# resource-pool profile vpdn profile32
Router(config-vpdn-profile)#  vpdn group l2tp
Router(config-vpdn-profile)#  vpdn group l2f
```

Related Commands

Command	Description
limit base-size	Defines the base number of simultaneous connections that can be done in a single customer or VPDN profile.
limit overflow-size	Defines the number of overflow calls granted to one customer or VPDN profile.
vpdn group	Associates a VPDN group with a customer or VPDN profile.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.
vpdn profile	Associates a VPDN profile with a customer profile.

service vpdn group

To provide virtual private dialup network (VPDN) service for the Subscriber Service Switch policy, use the **service vpdn group** command in subscriber profile configuration mode. To remove VPDN service, use the **no** form of this command.

service vpdn group *vpdn-group-name*

no service vpdn group *vpdn-group-name*

Syntax Description

vpdn-group-name	Provides the VPDN service by obtaining the configuration from a predefined VPDN group.

Command Default

This command is disabled by default.

Command Modes

Subscriber profile configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

The **service vpdn group** command provides VPDN service by obtaining the configuration from a predefined VPDN group for the SSS policy defined with the **subscriber profile** command.

Examples

The following example provides VPDN service to users in the domain cisco.com and uses VPDN group 1 to obtain VPDN configuration information:

```
!
subscriber profile cisco.com
 service vpdn group 1
```

The following example provides VPDN service to dialed number identification service (DNIS) 1234567 and uses VPDN group 1 to obtain VPDN configuration information:

```
!
subscriber profile dnis:1234567
 service vpdn group 1
```

The following example provides VPDN service using a remote tunnel (used on the multihop node) and uses VPDN group 1 to obtain VPDN configuration information:

```
!
```

```
subscriber profile host:lac
 service vpdn group 1
```

Related Commands

Command	Description
service deny	Denies service for the SSS policy.
service local	Enables local termination service for the SSS policy.
service relay	Enables relay of PAD messages over an L2TP tunnel.
subscriber profile	Defines the SSS policy for searches of a subscriber profile database.
vpdn-group	Associates a VPDN group to a customer or VPDN profile.

session-limit (VPDN)

To limit the number of simultaneous virtual private dialup network (VPDN) sessions allowed for a specified VPDN group, use the **session-limit** command in VPDN group configuration mode. To remove a configured session limit restriction, use the **no** form of this command.

session-limit *number*

no session-limit *number*

Syntax Description

number	Number of sessions allowed through a specified VPDN group. The range is 0 to 32767.

Command Default

No session limit exists for a VPDN group.

Command Modes

VPDN group configuration (config-vpdn)

Command History

Release	Modification
12.2(1)DX	This command was introduced.
12.2(2)DD	This command was integrated into Cisco IOS Release 12.2(2)DD.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(11)T	This command was implemented on the Cisco 1760, Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 platforms.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

Use this command to limit the number of allowed sessions for the specified VPDN group. If the **session-limit** command is configured to 0, no sessions are allowed on the VPDN group.

You must configure the VPDN group as either an accept dial-in or request dial-out VPDN subgroup before you can issue the **session-limit** command.

The maximum number of VPDN sessions can be configured globally by using the **vpdn session-limit** command, at the level of a VPDN group by using the **session-limit** 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 configures an accept dial-in VPDN group named group1 and restricts the VPDN group to a maximum of three simulataneous sessions:

```
Router(config)# vpdn-group group1
Router(config-vpdn)# accept-dialin
Router(config-vpdn-acc-in)# protocol l2tp
Router(config-vpdn-acc-in)# virtual-template 5
Router(config-vpdn-acc-in)# exit
Router(config-vpdn)# terminate-from hostname host1
Router(config-vpdn)# session-limit 3
```

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 dial-in VPDN subgroup configuration mode.
group session-limit	Limits the number of simultaneous VPDN sessions allowed across all VPDN groups associated with a particular VPDN template.
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.
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.

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.

set identifier (control policy-map class)

To create a temporary memory to hold the value of identifier types received by policy manager, use the **set identifier** command in configuration-control-policymap-class mode. To remove a temporary memory to hold the value of identifier types received by policy manager, use the **no** form of this command.

action number **set** *varname* **identifier** *type*

no *action number* **set** *varname* **identifier** *type*

Syntax Description

action-number	Number of the action. Actions are executed sequentially within the policy rule.
varname	Creates a temporary place in memory to store the value of the identifier type received by policy manager. Its scope is limited to the enclosing control class-map.
type	Specifies the type of identifier.

Command Modes

Configuration-control-policymap-class

Command History

Release	Modification
12.2(31)SB2	This command was introduced.

Usage Guidelines

The **set identifier** command allows you to create a temporary memory to hold the value of identifier types received by policy manager.

Examples

The following example shows the policy map with the set identifier statement 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
authenticate	Initiates an authentication request for an Intelligent Service Gateway (ISG) subscriber session.
substitute	Matches the contents, stored in temporary memory of identifier types received by policy manager, against a specified *matching-pattern* and performs the substitution defined in *rewrite-pattern.*

set variable (control policy-map class)

To create a temporary memory to hold the value of identifier types received by the policy manager, use the **set variable** command in configuration-control-policymap-class configuration mode. To remove a temporary memory to hold the value of identifier types received by the policy manager, use the **no** form of this command.

action-number **set** *variable* **identifier** *type*

no *action-number* **set** *variable* **identifier** *type*

Syntax Description

action-number	Number of the action. Actions are executed sequentially within the policy rule.
variable	Creates a temporary place in memory to store the value of the identifier type received by the policy manager. Its scope is limited to the enclosing control class map.
type	Specifies the type of identifier.

Command Default

The control policy is not affected.

Command Modes

Configuration-control-policymap-class configuration

Command History

Release	Modification
12.2(31)SB2	This command was introduced.

Usage Guidelines

The **set variable** command allows you to create a temporary memory to hold the value of identifier types received by the policy manager.

Examples

The following example shows the policy map with the set variable statement 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
authenticate	Initiates an authentication request for an ISG subscriber session.
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 *rewrite pattern.*

show interfaces virtual-access

To display status, traffic data, and configuration information about a specified virtual access interface, use the **show interfaces virtual-access** command in privileged EXEC mode.

show interfaces virtual-access *number* [**configuration**]

Syntax Description

number	Number of the virtual access interface.
configuration	(Optional) Restricts output to configuration information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.2F	This command was introduced.
11.3	The **configuration** keyword was added.
12.3(7)T	The output for this command was modified to indicate if the interface is a member of a multilink PPP bundle.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB. This command was implemented on the Cisco 10000 series router for the PRE3 and PRE4.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.3(33)SRE.

Usage Guidelines

To identify the number of the vty on which the virtual access interface was created, enter the **show users** command.

The counts of output packet bytes as reported by the L2TP access concentrator (LAC) to the RADIUS server in the accounting record do not match those of a client. The following paragraphs describe how the accounting is done and how you can determine the correct packet byte counts.

Packet counts for client packets in the input path are as follows:

- For packets that are process-switched, virtual access input counters are incremented by the coalescing function by the PPP over Ethernet (PPPoE) payload length.
- For packets that are fast-switched, virtual access input counters are incremented by the fast-switching function by the formula:

PPPoE payload length + PPP address&control bytes = = PPPoE payload length + 2

- For packets that are Cisco Express Forwarding switched, virtual access input counters are incremented by the Cisco Express Forwarding switching function by the formula:

IP length + PPP encapbytes (4) = = PPPoE payload length + 2

Packet counts for client packets in the output path are as follows:

- For packets that are process-switched by protocols other than PPP, virtual access output counters are incremented in the upper layer protocol by the entire datagram, as follows:

Size = PPPoE payload + PPPoE hdr (6) + Eth hdr (14) + SNAP hdr (10) + media hdr (4 for ATM)

- For packets process-switched by PPP Link Control Protocol (LCP) and Network Control Protocol (NCP), virtual access output counters are incremented by PPP, as follows:

PPP payload size + 4 bytes of PPP hdr

- For packets that are Cisco Express Forwarding fast-switched, virtual access counters are incremented by the PPPoE payload size.

Accounting is done for PPPoE, PPPoA PPP Termination Aggregation (PTA), and L2X as follows:

- For PPPoE PTA, the PPPoE payload length is counted for all input and output packets.
- For PPPoE L2X on a LAC, the PPPoE payload length is counted for all input packets. On an L2TP network server (LNS), the payload plus the PPP header (address + control + type) are counted.
- For PPP over ATM (PPPoA) PTA I/p packets, the payload plus the PPP address plus control bytes are counted. For PPPoA PTA o/p packets, the payload plus PPP address plus control plus ATM header are counted.
- For PPPoA L2X on a LAC for I/p packets, the payload plus PPP addr plus cntl bytes are counted. For PPPoA L2X on a LNS, the payload plus PPP header (address + control + type) are counted.

In Cisco IOS Release 12.2(33)SB and later releases, the router no longer allows you to specify a virtual access interface (VAI) as **vi** *x***.***y* in the **show pxf cpu queue** and **show interfaces** commands. Instead, you must spell out the VAI as **virtual-access**.

For example, when you enter the following commands, the router accepts the command:

```
Router# show interfaces virtual-access 2.1
```

In releases prior to Cisco IOS Release 12.2(33)SB, the router accepts the abbreviated form of the VAI. For example, the router accepts the following commands:

```
Router# show interfaces vi2.1
```

Examples

The following is sample output from the **show interfaces virtual-access** command:

```
Router# show interfaces virtual-access 3
Virtual-Access3 is up, line protocol is up
  Hardware is Virtual Access interface
  MTU 1500 bytes, BW 149760 Kbit, DLY 100000 usec,
     reliability 255/255, txload ½55, rxload ½55
  Encapsulation PPP, LCP Open, multilink Open
  Link is a member of Multilink bundle Virtual-Access4
  PPPoATM vaccess, cloned from Virtual-Template1
  Vaccess status 0x44
  Bound to ATM4/0.10000 VCD:16, VPI:15, VCI:200, loopback not set
  DTR is pulsed for 5 seconds on reset
  Last input never, output never, output hang never
  Last clearing of "show interfaces" counters 00:57:37
  Input queue:0/75/0/0 (size/max/drops/flushes); Total output drops:0
  Queueing strategy:fifo
  Output queue:0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     676 packets input, 12168 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     676 packets output, 10140 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
```

The table below describes the significant fields shown in the display.

Table 5 show interfaces virtual-access Field Descriptions

Field	Description
Virtual-Access ... is {up | down | administratively down}	Indicates whether the interface is currently active (whether carrier detect is present), is inactive, or has been taken down by an administrator.
line protocol is {up | down | administratively down}	Indicates whether the software processes that handle the line protocol consider the line to be usable (that is, whether keepalives are successful).
Hardware is	Type of interface. In this case, the interface is a dynamically created virtual access interface that exists on a vty line.
MTU	Maximum transmission unit for packets on the virtual access interface.
BW	Bandwidth of the virtual access interface, in kbps.
DLY	Delay of the virtual access interface, in microseconds.
reliability	Reliability of the virtual access interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over five minutes.
txload, rxload	Load on the virtual access interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes. The calculation uses the value from the **bandwidth** interface configuration command. • txload-- Transmit load on the virtual access interface as a value of ½55 calculated as an exponential average over 5 minutes. • rxload-- Receive load on the virtual access interface as a value of ½55 calculated as an exponential average over 5 minutes.

Field	Description
Encapsulation	Encapsulation method assigned to the virtual access interface.
loopback	Test in which signals are sent and then directed back toward the source at some point along the communication path. Used to test network interface usability.
DTR	Data terminal ready. An RS232-C circuit that is activated to let the DCE know when the DTE is ready to send and receive data.
LCP open | closed | req sent	Link Control Protocol (for PPP only; not for Serial Line Internet Protocol (SLIP)). LCP must come to the open state before any useful traffic can cross the link.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by a virtual access interface. This value indicates when a dead interface failed.
output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by a virtual access interface.
output hang	Number of hours, minutes, and seconds (or never) since the virtual access interface was last reset because of a transmission that took too long. When the number of hours in any of the "last" fields exceeds 24 hours, the number of days and hours is displayed. If that field overflows, asterisks are displayed.
Last clearing	Time at which the counters that measure cumulative statistics (such as number of bytes transmitted and received) were last reset to zero. Note that variables that might affect routing (for example, load and reliability) are not cleared when the counters are cleared. Asterisks (***) indicate that the elapsed time is too lengthy to be displayed. Zeros (0:00:00) indicate that the counters were cleared more than 231 milliseconds (ms) and less than 232 ms ago.
Input queue, drops	Number of packets in input queues. Each number is followed by a slash, the maximum size of the queue, and the number of packets dropped because of a full queue.

Field	Description
Queueing strategy	Type of queueing selected to prioritize network traffic. The options are first-come-first-served (FCFS) queueing, first-in-first-out queueing (FIFO), weighted fair queueing, priority queueing, and custom queueing.
Output queue	Packets in output queues. Represented by the maximum size of the queue followed by a slash and the number of packets dropped because of a full queue. For example, if the output queue is 45/15, 45 is the maximum size of the queue and 15 is the number of packets dropped.
5 minute input rate, 5 minute output rate	Average number of bits and packets transmitted per second in the last five minutes.
packets input	Total number of error-free packets received by the system.
bytes	Total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.
no buffer	Number of received packets discarded because there was no buffer space in the main system. Compare with ignored count. Broadcast storms on Ethernets and bursts of noise on serial lines are often responsible for no-input-buffer events.
broadcasts	Total number of broadcast or multicast packets received by the virtual access interface.
runts	Number of packets that are discarded because they are smaller than the medium's minimum packet size.
giants	Number of packets that are discarded because they exceed the medium's maximum packet size.
input errors	Total number of no-buffer, runts, giants, cyclic redundancy checks (CRCs), frame, overrun, ignored, and abort counts. Other input-related errors can also increment the count, so that this sum might not balance with the other counts.

Field	Description
CRC	Counter that reflects when the cyclic redundancy checksum generated by the originating LAN station or far-end device does not match the checksum calculated from data received. On a LAN, this often indicates noise or transmission problems on the LAN interface or the LAN bus. A high number of CRCs is usually the result of collisions or a station transmitting bad data. On a serial link, CRCs often indicate noise, gain hits, or other transmission problems on the data link.
frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets. On a serial line, this is usually the result of noise or other transmission problems.
overrun	Number of times the serial receiver hardware was unable to send received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.
ignored	Number of received packets ignored by the virtual access interface because the interface hardware ran low on internal buffers. These buffers are different from the system buffers mentioned in the description of the no buffer field. Broadcast storms and bursts of noise can cause the ignored count to be incremented.
abort	Illegal sequence of one bits on a virtual access interface. This usually indicates a clocking problem between the virtual access interface and the data link equipment.
packets output	Total number of messages transmitted by the system.
bytes	Total number of bytes, including data and MAC encapsulation, transmitted by the system.
underruns	Number of times the far-end transmitter has been running faster than the near-end communication server's receiver can handle. Underruns may never be reported on some virtual access interfaces.

Field	Description
output errors	Sum of all errors that prevented the final transmission of datagrams out of the virtual access interface being examined. Note that this might not balance with the sum of the enumerated output errors, because some datagrams might have more than one error, and others might have errors that do not fall into any of the tabulated categories.
collisions	Number of packets colliding.
interface resets	Number of times a virtual access interface has been completely reset. A reset can happen if packets queued for transmission were not sent within several seconds. Resetting can be caused by a malfunctioning modem that is not supplying the transmit clock signal or by a cable problem. If the system notices that the carrier detect line of a virtual access interface is up, but the line protocol is down, it periodically resets the interface in an effort to restart it. Interface resets can also occur when a virtual access interface is looped back or shut down.
output buffer failures	Number of outgoing packets dropped from the output buffer.
output buffers swapped out	Number of times the output buffer was swapped out.
carrier transitions	Number of times the carrier detect (CD) signal of a virtual access interface has changed state. Indicates modem or line problems if the CD line changes state often. If data carrier detect (DCD) goes down and comes up, the carrier transition counter increments two times.

Related Commands

Command	Description
clear interface virtual-access	Tears down the virtual access interface and frees the memory for other dial-in uses.
interface virtual-template	Creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces.
show pxf cpu queue	Displays PXF queueing statistics.

Command	Description
show users	Displays information about the active lines on the router or information about lawful-intercept users.

show l2tp class

To display information about Layer 2 Tunneling Protocol (L2TP) class, use the **show l2tp class** command in privileged EXEC mode.

show l2tp class

Syntax Description

This command has no arguments or keywords.

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

To use the **show l2tp class** command, you must configure these commands:

- The **vpdn enable** command in global configuration mode
- The **vpdn-group** command in global configuration mode
- The **request-dialin** command in VPDN group configuration mode
- The **protocol** command in request dial-in VPDN subgroup configuration mode
- The **domain** command in request dial-in VPDN subgroup configuration mode
- The **initiate-to** command in VPDN group configuration mode
- The **local name** command in VPDN group configuration mode
- The **l2tp tunnel password** command in VPDN group configuration mode
- The **l2tp attribute clid mask-method** command in VPDN group configuration mode

Examples

The following example shows how to configure an L2TP class using the preceding commands:

```
Router> enable
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# vpdn enable
Router(config)# vpdn-group l2tp
Router(config-vpdn)# request-dialin
Router(config-vpdn-req-in)# protocol l2tp
Router(config-vpdn-req-in)# domain cisco.com
Router(config-vpdn-req-in)# domain cisco.com#184
Router(config-vpdn-req-in)# exit
Router(config-vpdn)# initiate-to ip 10.168.1.4
Router(config-vpdn)# local name router32
Router(config-vpdn)# l2tp tunnel password 0 cisco
Router(config-vpdn)# l2tp attribute clid mask-method remove match #184
Router(config-vpdn)# exit
Router(config)# l2tp-class test
Router(config-l2tp-class)# exit
Router(config)# exit
```

The following is sample output from the **show l2tp class** command:

```
Router# show l2tp class
class [l2tp_default_class]
  is a statically configured class
  is not to be shown on running config
  is locked by:    "Exec" (1 time)
    "Internal" (1 time)
  configuration:
    l2tp-class l2tp_default_class
    !
class [test]
  is a statically configured class
  configuration:
    l2tp-class test
    !
```

The table below describes the significant fields shown in the display.

Table 6 show l2tp class Field Descriptions

Field	Description
l2tp_default_class	Name of the default L2TP class.
test	Name of the L2TP class.

Related Commands

Command	Description
domain (isakmp-group)	Specifies the DNS domain to which a group belongs and enters the (ISAKMP) group configuration mode.
initiate-to	Specifies an IP address used for Layer 2 tunneling.
local name	Specifies a local hostname that the tunnel uses to identify itself.
l2tp attribute clid mask-method	Configures a NAS to suppress L2TP calling station IDs for sessions associated with a VPDN group or VPDN template and enters a VPDN group or VPDN template configuration mode.
l2tp-class	Configures an L2TP class.
l2tp tunnel password	Sets the password the router uses to authenticate L2TP tunnels.

Command	Description
protocol (L2TP)	Specifies the signaling protocol to be used to manage the pseudowires created from a pseudowire class for a Layer 2 session and to cause control plane configuration settings to be taken from a specified L2TP class.
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.
vpdn enable	Enables VPDN on the router and informs the router to look for tunnel definitions in a local database and on a remote authorization server (home gateway), if one is present.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.

show l2tp counters

To display information about Layer 2 Tunneling Protocol (L2TP) counters and tunnel statistics, use the **show l2tp counters** command in privileged EXEC mode.

Cisco IOS Release 12.4(24)T and Later Releases

show l2tp counters tunnel [**all** | **authentication** | **id** *local-tunnel-id*]

Cisco IOS Release 12.2(33)SRC, Cisco IOS XE Release 2.1, and Later Releases

show l2tp counters {**session fsm** {**event** | **state** {**current** | **transition**}} [**icrq** | **manual** | **ocrq**] | **tunnel** [**all** | **authentication** | **id** *local-tunnel-id*]}

Syntax Description

tunnel	Specifies the L2TP tunnel counters.
all	(Optional) Displays the summary of all the tunnels with per-tunnel statistics.
authentication	(Optional) Specifies the tunnel authentication statistics.
id *local-tunnel-id*	(Optional) Specifies the local tunnel ID of the L2TP counter. The range is 1 to 4294967295.
session	Specifies the L2TP session counters.
fsm	Specifies the finite state machine counters.
event	Specifies the session event counters.
state	Specifies the session state counters.
current	Displays current counts of sessions in each state.
transition	Displays state machine transition counters.
icrq	(Optional) Specifies any one of the following state machine-related counters: • Incoming Call Request (ICRQ) • Incoming Call Reply (ICRP) • Incoming Call Connected (ICCN)
manual	(Optional) Specifies the manual session state machine-related counters.

ocrq	(Optional) Specifies any one of the following state machine-related counters: • Outgoing Call Request (OCRQ) • Outgoing Call Reply (OCRP) • Outgoing Call Connected (OCCN)

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. The **session**, **fsm**, **event**, **state**, **current**, **transition**, **icrq**, **manual**, and the **ocrq** keywords were added.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

To use the **show l2tp counters** command, you must configure these commands:

- The **vpdn enable** command in global configuration mode
- The **vpdn-group** command in global configuration mode
- The **request-dialin** command in VPDN group configuration mode
- The **protocol** command in appropriate VPDN subgroup configuration mode
- The **domain** command in request dial-in VPDN subgroup configuration mode
- The **initiate-to** command in VPDN group configuration mode
- The **local name** command in VPDN group configuration mode
- The **l2tp tunnel password** command in VPDN group configuration mode
- The **l2tp attribute clid mask-method** command in VPDN group configuration mode

Examples

The following is sample output from the **show l2tp counters** command:

```
Router# show l2tp counters tunnel
Global L2TP tunnel control message statistics:
                   XMIT      RE-XMIT         RCVD         DROP
                 ==========   ==========   ==========   ==========
ZLB                    0             0             0             0
SCCRQ                  6            10             0             0
SCCRP                  0             0             1             0
SCCCN                  1             0             0             0
StopCCN                5             5             0             0
Hello                  0             0             0             0
OCRQ                   0             0             0             0
```

```
OCRP                  0            0            0            0
OCCN                  0            0            0            0
ICRQ                  2            0            0            0
ICRP                  0            0            2            0
ICCN                  2            0            0            0
CDN                   0            0            0            0
WEN                   0            0            0            0
SLI                   2            0            4            0
EXP ACK               0            0            0            0
SRRQ                  0            0            0            0
SRRP                  0            0            0            0
CiscoACK              4            0            5            5
Total                32           25           22           15
```

The table below describes the significant fields shown in the display.

Table 7 show l2tp counters Field Descriptions

Field	Description
XMIT	The number of control messages that have been sent.
RE-XMIT	The number of control messages that have been sent.
RCVD	The number of control messages that have been received.
DROP	The number of control messages that have been dropped.
ZLB	The number of Zero Length Body (ZLB) messages.
SCCRQ	The number of Start-Control-Connection-Request (SCCRQ) messages.
SCCRP	The number of Start-Control-Connection-Reply (SCCRP) messages.
SCCCN	The number of Start-Control-Connection-Connected (SCCCN) messages.
StopCCN	The number of Stop-Control-Connection-Notification (StopCCN) messages.
Hello	The number of hello messages.
OCRQ	The number of Outgoing-Call-Request (OCRQ) messages.
OCRP	The number of Outgoing-Call-Reply (OCRP) messages.
OCCN	The number of Outgoing-Call-Connected (OCCN) messages.
ICRQ	The number of Incoming-Call-Request (ICRQ) messages.

Field	Description
ICRP	The number of Incoming-Call-Reply (ICRP) messages.
ICCN	The number of Incoming-Call-Connected (ICCN) messages.
CDN	The number of Call-Disconnect-Notify (CDN) messages.
WEN	The number of WAN-Error-Notify (WEN) messages.
SLI	The number of Set-Link-Info (SLI) messages.
EXP ACK	The number of Explicit-Acknowledgment (ACK) messages.
SRRQ	The number of Service Relay Request Message (SRRQ) messages.
SRRP	The number of Service Relay Reply Message (SRRP) messages.
CiscoACK	The number of Cisco Explicit-Acknowledgment (ACK) messages.

The following is sample output from the **show l2tp counters session** command:

```
Router# show l2tp counter session fsm state transition manual
Counters shown are for non-signaled, manual sessions only:

Old State                     New State

                     Idl      Wt      Wt    est    Dead
                              Soc     Loc   bli
                                      l     hed
                    =====   =====   =====   ===== =====
Init                 -        -       -      -      -
Idle                 -        -       -      -      -
Wt-Sock              -        -       -      -      -
Wt-Local             -        -       -      -      -
establish            -        -       -      -      -
Dead                 -        -       -      -      -
```

The table below describes the significant fields shown in the display.

Table 8 show l2tp counters Field Descriptions

Field	Description
Init	The state when memory associated with the control channel is not set.
Idle	The state when there is no application yet.

Field	Description
Wt-Sock	The state when L2X socket has been allocated and waiting for the socket to come up.
Wt-Local	The state of wait for the dataplane to come up.
establish	The state when the L2TP control channel is established.
Dead	The state when the session has transitioned to its terminal state and is about to be freed.

Related Commands

Command	Description
domain	Specifies the domain name of users that are to be forwarded to a tunnel server using a VPDN.
initiate-to	Specifies an IP address used for Layer 2 tunneling.
local name	Specifies a local hostname that the tunnel uses to identify itself.
l2tp attribute clid mask-method	Configures a NAS to suppress L2TP calling station IDs for sessions associated with a VPDN group or VPDN template and enters a VPDN group or VPDN template configuration mode.
l2tp tunnel password	Sets the password the router uses to authenticate L2TP tunnels.
protocol (VPDN)	Specifies the tunneling protocol used by a VPDN subgroup.
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.
show l2tp tunnel	Displays information about L2TP tunnels.
vpdn enable	Enables VPDN on the router and informs the router to look for tunnel definitions in a local database and on a remote authorization server (home gateway), if one is present.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.

show l2tp memory

To display information about Layer 2 Tunneling Protocol (L2TP) memory, use the **show l2tp memory** command in privileged EXEC mode.

show l2tp memory [**detail**]

Syntax Description

detail	(Optional) Displays details about L2TP memory usage.

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 **show l2tp memory** command to display information about L2TP memory.

To use the **show l2tp memory** command, you must configure these commands:

- The **vpdn enable** command in global configuration mode
- The **vpdn-group** command in global configuration mode
- The **request-dialin** command in VPDN group configuration mode
- The **protocol** command in request dial-in VPDN subgroup configuration mode
- The **domain** command in request dial-in VPDN subgroup configuration mode
- The **initiate-to** command in VPDN group configuration mode
- The **local name** command in VPDN group configuration mode
- The **l2tp tunnel password** command in VPDN group configuration mode
- The **l2tp attribute clid mask-method** command in VPDN group configuration mode

Examples

The following is sample output from the **show l2tp memory** command:

```
Router# show l2tp memory
  Allocator-Name                  In-use/Allocated            Count
  ----------------------------------------------------------------------------
  L2TP AVP chunk            :     16960/18232      ( 93%) [    212] Chunk
  L2TP AVP vendor+type      :        24/76         ( 31%) [      1]
  L2TP AVP vendor+type+app  :        24/76         ( 31%) [      1]
  L2TP AVPs                 :        52/104        ( 50%) [      1]
  L2TP CC Author DB         :         0/32820      (  0%) [      0] Chunk
  L2TP CC ID                :        24/76         ( 31%) [      1]
  L2TP CC ublock            :         0/65588      (  0%) [      0] Chunk
  L2TP CLID mask match      :        44/96         ( 45%) [      1]
  L2TP DB                   :        36/65640      (  0%) [      1] Chunk
  L2TP Event Msg chunks     :         0/65588      (  0%) [      0] Chunk
  L2TP ISSU Session         :       532/792        ( 67%) [      5]
  L2TP L2X CC DB            :     65780/65936      ( 99%) [      3]
  L2TP L2X SESSION DB       :     83764/83920      ( 99%) [      3]
  L2TP L2X cc chunk         :         0/65588      (  0%) [      0] Chunk
  L2TP L2X sn chunk         :         0/65588      (  0%) [      0] Chunk
  L2TP SN ID                :         0/65588      (  0%) [      0] Chunk
  L2TP SN INT ID            :         0/65588      (  0%) [      0] Chunk
  L2TP SN V2 ID             :        24/76         ( 31%) [      1]
  L2TP SN V3 ID             :        36/88         ( 40%) [      1]
  L2TP Socket Msg chunks    :         0/4304       (  0%) [      0] Chunk
  L2TP mgd timer chunk      :         0/65588      (  0%) [      0] Chunk
  L2TP v3 L3VPN Session ID  :        96/148        ( 64%) [      1]
  L2TUN DISC DB             :         0/32820      (  0%) [      0] Chunk
  L2TUN discovery sess chun :         0/576        (  0%) [      0] Chunk
  L2TUN discovery sess chun :         0/1552       (  0%) [      0] Chunk
  L2X CC ublock             :        88/140        ( 62%) [      1]
  L2X Hash Table            :   2097152/2097204    ( 99%) [      1]
  L2X SN ublock             :        88/140        ( 62%) [      1]
  L2X Sn DB entries chunk   :         0/65588      (  0%) [      0] Chunk
  L2X Sw Sn chunk           :         0/65588      (  0%) [      0] Chunk
  L2X author chunk          :         0/65588      (  0%) [      0] Chunk
  L2X author ctx            :       212/264        ( 80%) [      1]
  L2X author hdr chunk      :         0/18232      (  0%) [      0] Chunk
  L2X cc author db          :        32/84         ( 38%) [      1]
  Total allocated: 2.936 Mb, 3007 Kb, 3079276 bytes
```

The table below describes the significant fields shown in the display.

Table 9 show l2tp memory Field Descriptions

Field	Description
Allocator-Name	Name of the counters that allocated the block.
In-use/Allocated	Number of bytes in use and the number of bytes allocated for use by L2TP, L2TUN, and L2X counters.
Count	Number of blocks in use.
Total allocated	Memory, allocated in bytes.

Related Commands

Command	Description
domain (isakmp-group)	Specifies the DNS domain to which a group belongs and enters the ISAKMP group configuration mode.
initiate-to	Specifies an IP address used for Layer 2 tunneling.

Command	Description
local name	Specifies a local hostname that the tunnel uses to identify itself.
l2tp attribute clid mask-method	Configures a NAS to suppress L2TP calling station IDs for sessions associated with a VPDN group or VPDN template and enters a VPDN group or VPDN template configuration mode.
l2tp tunnel password	Sets the password the router uses to authenticate L2TP tunnels.
protocol (L2TP)	Specifies the signaling protocol to be used to manage the pseudowires created from a pseudowire class for a Layer 2 session and to cause control plane configuration settings to be taken from a specified L2TP class.
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.
show l2tp tunnel	Displays information about L2TP tunnels.
show l2tp counters	Displays information about L2TP counters and tunnel statistics.
vpdn enable	Enables VPDN on the router and informs the router to look for tunnel definitions in a local database and on a remote authorization server (home gateway), if one is present.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.

show l2tp redundancy

To display information about a Layer 2 Tunneling Protocol (L2TP) high availability (HA) stateful switchover (SSO) session, including its state, use the **show l2tp redundancy** command in privileged EXEC mode.

show l2tp redundancy [**all** | [**detail**] [**id** *local-tunnel-ID* [*local-session-ID*]]]

Syntax Description

all	(Optional) Displays a summary of all L2TP redundancy data.
detail	(Optional) Displays detailed information about L2TP redundancy.
id	(Optional) Displays redundancy information about the specified local tunnel or local session.
local-tunnel-ID	(Optional) Displays redundancy information about the specified local session. The range is 1 to 4294967295.
local-session-ID	(Optional) Displays redundancy information about the specified local tunnel. The range is 1 to 4294967295.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.2	This command was introduced.
Cisco IOS XE Release 3.3S	This command was modified. The **show l2tp redundancy detail** command output was enhanced to provide counters for tunnels and sessions cleared during the resynchronization phase. The **show l2tp redundancy** command output was enhanced to show whether the resynchronization has started or not started.

Usage Guidelines

The **show l2tp redundancy** command displays the same information as the **show vpdn redundancy** command.

During the time frame immediately after a switchover and before the resynchronization starts, if you enter the **show l2tp redundancy** command, the last line of the command output is "Resync not yet started."

Once the resynchronization starts, the line "L2TP Resynced Tunnels: 0/0 (success/fail)" is shown. When the resynchronization completes, the "Resync duration 0.0 secs (complete)" is shown.

Examples

The following example shows how to display the global status of L2TP redundancy information:

```
Router# show l2tp redundancy
L2TP HA support: Silent Failover
L2TP HA Status:
  Checkpoint Messaging on: TRUE
  Standby RP is up:        TRUE
  Recv'd Message Count:    189
  L2TP Tunnels:            2/2/2/0 (total/HA-enabled/HA-est/resync)
  L2TP Sessions:           20/20/20 (total/HA-enabled/HA-est)
  L2TP Resynced Tunnels:   2/0 (success/fail)
  Resync duration 0.63 secs (complete)
```

The following example shows how to display a summary of all L2TP redundancy information:

```
Router# show l2tp redundancy all
L2TP HA support: Silent Failover
L2TP HA Status:
 Checkpoint Messaging on:                            FALSE
 Standby RP is up:                            TRUE
 Recv’d Message Count:                            0
 L2TP Active Tunnels:                            1/1 (total/HA-enable)
 L2TP Active Sessions:                            2/2 (total/HA-enable)
L2TP HA CC Check Point Status:
State            LocID        RemID        Remote Name                Class/
Group                            Num/Sessions
est            44233        51773        LNS                VPDN Group 1
10.1.1.1                            2
L2TP HA Session Status:
LocID        RemID        TunID            Waiting for                    Waiting for
                            VPDN app?                    L2TP proto?
2        2        44233            No                    No
2        3        44233            No                    No
```

The following example shows how to limit the displayed redundancy information to only the sessions associated with a specified tunnel ID:

```
Router# show l2tp redundancy id 44233
L2TP HA Session Status:
LocID        RemID        TunID            Waiting for                    Waiting for
                            VPDN app?                    L2TP proto?
2        2        44233            No                    No
2        3        44233            No                    No
```

The table below describes the significant fields shown in the **show l2tp redundancy**, **show l2tp redundancy all**, **show l2tp redundancy id**, and in the **show l2tp redundancy detail** command outputs.

Table 10 show l2tp redundancy Command Field Descriptions

Field	Description
Checkpoint Messaging on	Operational status of the checkpoint messaging infrastructure.
Standby RP is up	Operational status of the standby Route Processor (RP).

Field	Description
Recv'd Message Count	Number of checkpoint messages received on this RP.
L2TP Tunnels	Operational status of L2TP HA tunnels: • total--Number of L2TP tunnels operating on this router. • HA-enabled--Number of L2TP tunnels currently configured to be checkpointed to the standby RP. • HA-est--Number of HA tunnels currently established (as opposed to configured). • resync--Number of tunnels currently being resynchronized (usually during a switchover event).
L2TP Sessions	Operational status of L2TP HA sessions: • total--Number of L2TP sessions operating on this router. • HA-enabled--Number of L2TP sessions currently configured to be checkpointed to the standby RP. • HA-est--Number of HA sessions currently established (as opposed to configured).
L2TP Resynced Tunnels	Number of successful and failed L2TP resynchronized tunnels.
Resync duration	How long the resynchronization took, in seconds.
L2TP HA CC Check Point Status	
State	Status of the tunnel.
LocID	Local ID of the L2TP HA tunnel.
RemID	Remote tunnel ID.
Remote Name	Router name associated with this tunnel.
Class/Group	Unique number associated with the class or group as defined in the L2TP or VPDN configuration.
Num/Sessions	Number of sessions currently set up over the tunnel or CC.
Waiting for VPDN app	Status of the virtual private dialup network (VPDN) application checkpointing delay. The VPDN application checkpointing could delay the completion of the session setup.

Field	Description
Waiting for L2TP proto	Status of the L2TP protocol checkpointing delay. The L2TP protocol checkpointing could delay the completion of the session setup.
Tunnels destroyed during tunnel resync phase	
Poisoned	Number of L2TP tunnels poisoned during the resynchronization phase.
Failed to transmit the initial probe	Number of L2TP tunnels where the initial probe packet could not be transmitted during the resynchronization phase.
Cleared by peer	Number of L2TP tunnels cleared by the peer during the resynchronization phase.
Cleared due to excessive retransmits	Number of L2TP tunnels cleared due to an excessive number of probe retransmissions during the resynchronization phase.
Cleared because unestablished	Number of L2TP tunnels cleared because they were not completely established at the start of the resynchronization phase.
Cleared by us, other	Number of L2TP tunnels cleared for other reasons during the resynchronization phase.
Total	Total number of tunnels destroyed during the resynchronization phase.
Sessions destroyed during tunnel resync phase	
Poisoned	Number of L2TP sessions poisoned during the resynchronization phase.
Unestablished	Number of L2TP sessions cleared because they not completely established at the start of the resynchronization phase.
Missing application session	Number of L2TP sessions cleared because no corresponding VPDN session is at the end of the resynchronization phase.
Cleared by peer	Number of L2TP sessions cleared by the peer during the resynchronization phase.
Attempted before or during resync	Number of L2TP sessions attempted by the peer (after failover) before or during the resynchronization phase.

Field	Description
Tunnel poisoned	Number of L2TP sessions cleared because the tunnel carrying them was poisoned during the resynchronization phase.
Tunnel failed to transmit initial probe	Number of L2TP sessions cleared because the initial probe packet could not be transmitted on the tunnel.
Tunnel cleared by peer	Number of L2TP sessions cleared because the tunnel carrying them was cleared by the peer.
Tunnel cleared due to excessive retransmits	Number of L2TP sessions cleared because of an excessive number of retransmissions on the tunnel carrying them.
Tunnel cleared because unestablished	Number of L2TP sessions cleared because the tunnel carrying them was not completely established at the start of the resynchronization phase.
Tunnel cleared by us, other	Number of L2TP sessions cleared because the tunnel carrying them was cleared for some reason.
Sessions cleared, other	Number of sessions cleared for other reasons during the resynchronization phase.
Total	Total number of sessions destroyed during the resynchronization phase.

The following example shows how to limit the information displayed by providing a tunnel ID:

```
Router# show l2tp redundancy id 44233
 L2TP HA Session Status:
LocID        RemID        TunID            Waiting for                    Waiting for
                            VPDN app?                     L2TP proto?
2        2        44233            No                    No
```

The following example shows how to limit the information displayed by providing a session ID:

```
Router# show l2tp redundancy detail id 44233 3
Local session ID                                : 3
 Remote session ID                                : 3
 Local CC ID                                : 44233
 Local UDP port                                 : 1701
 Remote UDP port                                : 1701
 Waiting for VPDN application                                 : No
 Waiting for L2TP protocol                                 : No
```

The following example shows the detailed information displayed on a router newly active after a failover:

```
Router# show l2tp redundancy detail
L2TP HA Status:
  Checkpoint Messaging on: TRUE
  Standby RP is up:        TRUE
  Recv'd Message Count:    219
  L2TP Tunnels:            1/1/1/0 (total/HA-enabled/HA-est/resync)
  L2TP Sessions:           1/1/1 (total/HA-enabled/HA-est)
  L2TP Resynced Tunnels:   1/0 (success/fail)
  Resync duration 3.0 secs (complete)
```

```
Our Ns checkpoints: 0, our Nr checkpoints: 0
Peer Ns checkpoints: 0, peer Nr checkpoints: 0
Packets received before entering resync phase: 0
Nr0 adjusts during resync phase init: 0
Nr learnt from peer during resync phase: 0
Tunnels destroyed during tunnel resync phase
  Poisoned:                                  1
  Failed to transmit the initial probe:      2
  Cleared by peer:                           3
  Cleared due to excessive retransmits:      4
  Cleared because unestablished:             5
  Cleared by us, other:                      6
Total:                                      21
Sessions destroyed during tunnel resync phase
  Poisoned:                                        7
  Unestablished:                                   8
  Missing application session:                     9
  Cleared by peer:                                10
  Attempted before or during resync:              11
  Tunnel poisoned:                                12
  Tunnel failed to transmit initial probe:        13
  Tunnel cleared by peer:                         14
  Tunnel cleared due to excessive retransmits:    15
  Tunnel cleared because unestablished:           16
  Tunnel cleared by us, other:                    17
  Sessions cleared, other:                        18
Total:                                           134
```

Related Commands

Command	Description
debug l2tp redundancy	Displays information on L2TP sessions having checkpoint events and errors.
debug vpdn redundancy	Displays information on VPDN sessions having checkpoint events and errors.
l2tp sso enable	Enables L2TP HA.
l2tp tunnel resync	Specifies the number of packets sent before waiting for an acknowledgment message.
show vpdn redundancy	Displays VPDN redundancy information.
sso enable	Enables L2TP HA for VPDN groups.

show l2tp session

To display information about Layer 2 Tunneling Protocol (L2TP) sessions, use the **show l2tp session** command in privileged EXEC mode.

show l2tp session[**all** | **packets** [**ipv6**] | **sequence** | **state** | **brief** | **circuit** | **interworking**] [**hostname** | **ip-address** *ip-address* [**hostname** | **vcid** *vcid*] | **tunnel**{**id** *local-id* [*local-session-id*] | **remote-name** *remote-name local-name*} | **username** *username* | **vcid** *vcid*]

Syntax Description

all	(Optional) Displays information for all active sessions.
packets	(Optional) Displays information about packet or byte counts for sessions.
ipv6	(Optional) (Optional) Displays IPv6 packet and byte-count statistics.
sequence	(Optional) Displays sequence information for sessions.
state	(Optional) Displays state information for sessions.
brief	(Optional) Displays brief session information.
circuit	(Optional) Displays the Layer 2 circuit information.
interworking	(Optional) Displays interworking information.
hostname	(Optional) Displays output using L2TP control channel hostnames rather than IP addresses
ip-addr *ip-addr*	(Optional) Specifies the peer IP address associated with the session.
vcid *vcid*	(Optional) Specifies the Virtual Circuit ID (VCID) associated with the session. The range is 1 to 4294967295.
tunnel	(Optional) Displays the sessions in a tunnel.
id *local-tunnel-id local-session-id*	Specifies the session by tunnel ID and session ID. The range for the local tunnel ID and local session ID is 1 to 4294967295.
remote-name *remote-tunnel-name local-tunnel-name*	Specifies the remote names for the remote and local L2TP tunnels.
username *username*	(Optional) Specifies the username associated with the session.

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.
Cisco IOS XE Release 2.6	The **ipv6** keyword was added. The **show l2tp session** command with the **all** keyword was modified to display IPv6 counter information.

Usage Guidelines

To use the **show l2tp session** command, you must configure these commands:

- The **vpdn enable** command in global configuration mode
- The **vpdn-group** command in global configuration mode
- The **request-dialin** command in VPDN group configuration mode
- The **protocol** command in request dial-in VPDN subgroup configuration mode
- The **domain** command in request dial-in VPDN subgroup configuration mode
- The **initiate-to** command in VPDN group configuration mode
- The **local name** command in VPDN group configuration mode
- The **l2tp tunnel password** command in VPDN group configuration mode
- The **l2tp attribute clid mask-method** command in VPDN group configuration mode

Examples

The following is sample output from the **show l2tp session** command:

```
Router# show l2tp session packets
L2TP Session Information Total tunnels 1 sessions 2
LocID      RemID      TunID      Pkts-In    Pkts-Out   Bytes-In   Bytes-Out
18390      313101640  4059745793 0          0          0          0
25216      4222832574 4059745793 15746      100000     1889520    12000000
```

Related Commands

Command	Description
domain (isakmp-group)	Specifies the DNS domain to which a group belongs and enters the ISAKMP group configuration mode.
initiate-to	Specifies an IP address used for Layer 2 tunneling.

Command	Description
local name	Specifies a local hostname that the tunnel uses to identify itself.
l2tp attribute clid mask-method	Configures a NAS to suppress L2TP calling station IDs for sessions associated with a VPDN group or VPDN template and enters a VPDN group or VPDN template configuration mode.
l2tp tunnel password	Sets the password the router uses to authenticate L2TP tunnels.
protocol (L2TP)	Specifies the signaling protocol to be used to manage the pseudowires created from a pseudowire class for a Layer 2 session and to cause control plane configuration settings to be taken from a specified L2TP class.
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.
vpdn enable	Enables VPDN on the router and informs the router to look for tunnel definitions in a local database and on a remote authorization server (home gateway), if one is present.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.

show l2tp tunnel

To display details about Layer 2 Tunneling Protocol (L2TP) tunnels, use the **show l2tp tunnel** command in privileged EXEC mode.

show l2tp tunnel [**all** | **packets** [**ipv6**] | **state** | **summary** | **transport**] [**id** *local-tunnel-id* | **local-name** *local-tunnel-name remote-tunnel-name* | **remote-name** *remote-tunnel-name local-tunnel-name*]

Syntax Description

all	(Optional) Displays information about all active tunnels.
packets	(Optional) Displays information about packet or byte counts.
ipv6	(Optional) Displays IPv6 packet and byte-count statistics.
state	(Optional) Displays the state of the tunnel.
summary	(Optional) Displays a summary of the tunnel information.
transport	(Optional) Displays tunnel transport information.
id *local-tunnel-id*	(Optional) Specifies the local tunnel ID of the L2TP tunnel. The range is 1 to 4294967295.
local-name *local-tunnel-name remote-tunnel-name*	(Optional) Specifies the local names for the local and remote L2TP tunnels.
remote-name *remote-tunnel-name local-tunnel-name*	(Optional) Specifies the remote names for the remote and local L2TP tunnels.

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.

Release	Modification
Cisco IOS XE Release 2.6	The **ipv6** keyword was added. The **show l2tp tunnel** command with the **all** keyword was modified to display IPv6 counter information.

Usage Guidelines

To use the **show l2tp tunnel** command, you must configure these commands:

- The **vpdn enable** command in global configuration mode
- The **vpdn-group** command in global configuration mode
- The **request-dialin** command in VPDN group configuration mode
- The **protocol** command in request dial-in VPDN subgroup configuration mode
- The **domain** command in request dial-in VPDN subgroup configuration mode
- The **initiate-to** command in VPDN group configuration mode
- The **local name** command in VPDN group configuration mode
- The **l2tp tunnel password** command in VPDN group configuration mode
- The **l2tp attribute clid mask-method** command in VPDN group configuration mode

Depending on the keywords or arguments entered, the **show l2tp tunnel** command displays information such as packet or byte count, state, transport, local or remote names, and summary information for L2TP tunnels.

Examples

The following is sample output from the **show l2tp tunnel** command:

```
Router# show l2tp tunnel all
L2TP Tunnel Information Total tunnels 1 sessions 1 Tunnel id 746420372 is up, remote id
is 2843347489, 1 active sessions
 Remotely initiated tunnel
 Tunnel state is established, time since change 00:30:16  Tunnel transport is IP (115)
 Remote tunnel name is 7604-AA1705
  Internet Address 12.27.17.86, port 0
 Local tunnel name is 7606-AA1801
  Internet Address 12.27.18.86, port 0
 L2TP class for tunnel is l2tp_default_class
 Counters, taking last clear into account:
  598 packets sent, 39 received
  74053 bytes sent, 15756 received
  Last clearing of counters never
 Counters, ignoring last clear:
  598 packets sent, 39 received
  74053 bytes sent, 15756 received
 Control Ns 3, Nr 35
 Local RWS 1024 (default), Remote RWS 1024
 Control channel Congestion Control is disabled
 Tunnel PMTU checking disabled
 Retransmission time 1, max 1 seconds
 Unsent queuesize 0, max 0
 Resend queuesize 0, max 1
 Total resends 0, ZLB ACKs sent 33
 Total out-of-order dropped pkts 0
 Total out-of-order reorder pkts 0
 Total peer authentication failures 0
 Current no session pak queue check 0 of 5
 Retransmit time distribution: 0 0 0 0 0 0 0 0 0
 Control message authentication is disabled
```

Related Commands

Command	Description
domain (isakmp-group)	Specifies the DNS domain to which a group belongs and enters the ISAKMP group configuration mode.
initiate-to	Specifies an IP address used for Layer 2 tunneling.
local name	Specifies a local hostname that the tunnel uses to identify itself.
l2tp attribute clid mask-method	Configures a NAS to suppress L2TP calling station IDs for sessions associated with a VPDN group or VPDN template and enters a VPDN group or VPDN template configuration mode.
l2tp tunnel password	Sets the password the router uses to authenticate L2TP tunnels.
protocol (L2TP)	Specifies the signaling protocol to be used to manage the pseudowires created from a pseudowire class for a Layer 2 session and to cause control plane configuration settings to be taken from a specified L2TP class.
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.
vpdn enable	Enables VPDN on the router and informs the router to look for tunnel definitions in a local database and on a remote authorization server (home gateway), if one is present.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.

show ppp mppe

To display Microsoft Point-to-Point Encryption (MPPE) information for an interface, use the **show ppp mppe** command in privileged EXEC mode.

show ppp mppe {**serial** | **virtual-access**} [*number*]

Syntax Description

serial	Displays MPPE information for all serial interfaces.
virtual-access	Displays MPPE information for all virtual-access interfaces.
number	(Optional) Specifies an interface number. Restricts the display to MPPE information for only the specified interface number.

Command Modes

Privileged EXEC (#)

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

None of the fields in the output from the **show ppp mppe** command are fatal errors. Excessive packet drops, misses, out of orders, or CCP-Resets indicate that packets are getting lost. If you see such activity and have stateful MPPE configured, you might want to consider switching to stateless mode.

Examples

The following example displays MPPE information for virtual-access interface 3:

```
Router# show ppp mppe virtual-access 3
Interface Virtual-Access3 (current connection)
  Hardware (ISA5/1, flow_id=13) encryption, 40 bit encryption, Stateless mode
  packets encrypted = 0        packets decrypted  = 1
  sent CCP resets   = 0        receive CCP resets = 0
  next tx coherency = 0        next rx coherency  = 0
  tx key changes    = 0        rx key changes     = 0
  rx pkt dropped    = 0        rx out of order pkt= 0
  rx missed packets = 0
```

To update the key change information, reissue the **show ppp mppe virtual-access 3** command:

```
Router# show ppp mppe virtual-access 3
```

```
Interface Virtual-Access3 (current connection)
  Hardware (ISA5/1, flow_id=13) encryption, 40 bit encryption, Stateless mode
  packets encrypted = 0        packets decrypted  = 1
  sent CCP resets   = 0        receive CCP resets = 0
  next tx coherency = 0        next rx coherency  = 0
  tx key changes    = 0        rx key changes     = 1
  rx pkt dropped    = 0        rx out of order pkt= 0
  rx missed packets = 0
```

The table below describes the significant fields shown in the displays.

Table 11 show ppp mppe Field Descriptions

Field	Description
packets encrypted	Number of packets that have been encrypted.
packets decrypted	Number of packets that have been decrypted.
sent CCP resets	Number of CCP-Resets sent. One CCP-Reset is sent for each packet loss that is detected in stateful mode. When using stateless MPPE, this field is always zero.
next tx coherency	The coherency count (the sequence number) of the next packet to be encrypted.
next rx coherency	The coherency count (the sequence number) of the next packet to be decrypted.
key changes	Number of times the session key has been reinitialized. In stateless mode, the key is reinitialized once per packet. In stateful mode, the key is reinitialized every 256 packets or when a CCP-Reset is received.
rx pkt dropped	Number of packets received and dropped. A packet is dropped because it is suspected of being a duplicate or already received packet.
rx out of order pkt	Number of packets received that are out of order.

Related Commands

Command	Description
encryption mppe	Enables MPPE encryption on the virtual template.
pptp flow-control static-rtt	Specifies the timeout interval of the tunnel server between sending a packet to the client and receiving a response.

show resource-pool vpdn

To display information about a specific virtual private dialup network (VPDN) group or specific VPDN profile, use the **show resource-pool vpdn** command in privileged EXEC mode.

show resource-pool vpdn [{**group** | **profile** }**name**]

Syntax Description

group	All the VPDN groups configured on the router.
profile	All the VPDN profiles configured on the router.
name	(Optional) Specific VPDN group or profile.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

Use the **show resource-pool vpdn group** command to display information about a specific VPDN group.

Example 1

This example displays specific information about the VPDN group named vpdng2:

```
Router# show resource-pool vpdn group vpdng2
VPDN Group vpdng2 found under Customer Profiles: customer2
Tunnel (L2TP)
--------
dnis:customer2-calledg
cisco.com
Endpoint        Session Limit Priority Active Sessions Status Reserved Sessions
--------        ------------- -------- --------------- ------ -----------------
172.21.9.97     *             1        0               OK
                -------------          ---------------        -----------------
Total           *                      0                      0
```

Example 2

The following example displays information about all the VPDN groups configured on the router:

```
Router# show resource-pool vpdn group
List of VPDN Groups under Customer Profiles
Customer Profile customer1: vpdng1
Customer Profile customer2: vpdng2
List of VPDN Groups under VPDN Profiles
VPDN Profile profile1: vpdng1
VPDN Profile profile2: vpdng2
```

The table below describes the significant fields shown in the displays.

Table 12 *show resource-pool vpdn group Field Descriptions*

Field	Description
Endpoint	IP address of HGW/LNS router.
Session Limit	Number of sessions permitted for the designated endpoint.
Priority	Loadsharing HGW/LNSs are always marked with a priority of 1.
Active Sessions	Number of active sessions on the network access server. These are sessions successfully established with endpoints (not reserved sessions).
Status	Only two status types are possible: OK and busy.
Reserved Sessions	Authorized sessions that are waiting to see if they can successfully connect to endpoints. Essentially, these sessions are queued calls. In most cases, reserved sessions become active sessions.
*	No limit is set.
List of VPDN Groups under Customer Profiles	List of VPDN groups that are assigned to customer profiles. The customer profile name is listed first, followed by the name of the VPDN group assigned to it.
List of VPDN Groups under VPDN Profiles	List of VPDN groups that are assigned to VPDN profiles. The VPDN profile name is listed first, followed by the VPDN group assigned to it.

Example 3

The following example displays a list of all VPDN profiles configured on the router:

```
Router# show resource-pool vpdn profile
% List of VPDN Profiles:
profile1
profile2
profile3
```

Example 4

The following example displays details about a specific VPDN profile named vpdnp1:

```
Router# show resource-pool vpdn profile vpdnp1
        0 active connections
        0 max number of simultaneous connections
        0 calls rejected due to profile limits
        0 calls rejected due to resource unavailable
        0 overflow connections
        0 overflow states entered
        0 overflow connections rejected
        3003 minutes since last clear command
```

The table below describes the significant fields shown in the displays.

Table 13 show resource-pool vpdn profile Field Descriptions

Field	Description
List of VPDN Profiles	List of the VPDN profiles that have been assigned.
Active connections	Number of active VPDN connections counted by the VPDN profile.
Max number of simultaneous connections	Maximum number of VPDN simultaneous connections counted by the VPDN profile. This value helps you determine how many VPDN sessions to subscribe to a specific profile.
Calls rejected due to profile limits	Number of calls rejected since the last **clear** command because the profile limit has been exceeded.
Calls rejected due to resource unavailable	Number of calls rejected since the last **clear** command because the assigned resource was unavailable.
Overflow connections	Number of overflow connections used since the last **clear** command.
Overflow states entered	Number of overflow states entered since the last **clear** command.
Overflow connections rejected	Number of overflow connections rejected since the last **clear** command.
Minutes since last clear command	Number of minutes elapsed since the last **clear** command was used.

Related Commands

Command	Description
resource-pool profile customer	Creates a customer profile and enters customer profile configuration mode.
resource-pool profile vpdn	Creates a VPDN profile and enters VPDN profile configuration mode.
vpdn group	Associates a VPDN group with a customer or VPDN profile.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.

show vpdn

To display basic information about all active virtual private dialup network (VPDN) tunnels, use the **show vpdn** command in user EXEC or in privileged EXEC mode.

show vpdn

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
11.2	This command was introduced.
12.1(1)T	This command was enhanced to display PPP over Ethernet (PPPoE) information.
12.1(2)T	This command was enhanced to display PPPoE session information on actual Ethernet interfaces.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

Use the **show vpdn** command to display information about all active tunnels using Layer 2 Tunneling Protocol (L2TP), Layer 2 Forwarding (L2F), and Point-to-Point Tunnel Protocol (PPTP).

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

The output of the **show vpdn session** command also displays PPPoE session information. PPPoE is supported on ATM permanent virtual connections (PVCs) compliant with RFC 1483 only. PPPoE is not supported on Frame Relay and any other LAN interfaces such as FDDI and Token Ring.

Examples

The following is sample output from the **show vpdn** command on a device with active L2F and L2TP tunnels:

```
Router> show vpdn

Active L2F tunnels
NAS Name   Gateway Name    NAS CLID   Gateway CLID   State
```

```
nas        gateway           4            2          open
L2F MIDs
Name                    NAS Name    Interface    MID      State
router1@cisco.com       nas          As7          1       open
router2@cisco.com       nas          As8          2       open
%No active PPTP tunnels
```

The following is sample output from the **show vpdn** command on a device with an active PPPoE tunnel:

```
Router> show vpdn

%No active L2TP tunnels
%No active L2F tunnels
PPPoE Tunnel and Session Information Total tunnels 1 sessions 1
PPPoE Tunnel Information
Session count:1
PPPoE Session Information
SID        RemMAC          LocMAC       Intf    VASt    OIntf    VC
1       0010.7b01.2cd9  0090.ab13.bca8  Vi4     UP      AT6/0   0/104
```

The following is sample output from the **show vpdn** command on a device with an active PPPoE session on an Ethernet interface:

```
Router> show vpdn

%No active L2TP tunnels
%No active L2F tunnels

PPPoE Tunnel and Session Information Total tunnels 1 sessions 1
PPPoE Tunnel Information
Session count:1
PPPoE Session Information
SID        RemMAC          LocMAC       Intf    VASt    OIntf
1       0090.bf06.c870 00e0.1459.2521   Vi1      UP     Eth1
```

The table below describes the significant fields shown in the displays.

Table 14 show vpdn Field Descriptions

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

Field	Description
NAS Name	Hostname of the NAS.
Interface	Interface from which the protocol message was sent.
MID	Nmber uniquely identifying this user in this tunnel.
State	Indicates status for the individual user in the tunnel. The states are: opening, open, closing, closed, and waiting_for_tunnel. The waiting_for_tunnel state means that the user connection is waiting until the main tunnel can be brought up before it moves to the opening state.
PPPoE Tunnel Information	
SID	Session ID for the PPPoE session.
RemMAC	Remote MAC address of the host.
LocMAC	Local MAC address of the router. It is the default MAC address of the router.
Intf	Virtual access interface associated with the PPP session.
VASt	Line protocol state of the virtual access interface.
OIntf	Outgoing interface.
VC	VC on which the PPPoE session is established.

Related Commands

Command	Description
show vpdn domain	Displays all VPDN domains and DNIS groups configured on the NAS.
show vpdn group	Displays a summary of the relationships among VPDN groups and customer/VPDN profiles, or summarizes the configuration of a VPDN group including DNIS/domain, load sharing information, and current session information.
show vpdn history failure	Displays the content of the failure history table.
show vpdn multilink	Displays the multilink sessions authorized for all VPDN groups.
show vpdn redirect	Displays statistics for L2TP redirects and forwards.

Command	Description
show vpdn session	Displays session information about active Layer 2 sessions for a VPDN.
show vpdn tunnel	Displays information about active Layer 2 tunnels for a VPDN.

show vpdn dead-cache

To display a list of VPDN dead-cache state L2TP Network Servers (LNSs), use the **show vpdn dead-cache** command in user EXEC or in privileged EXEC mode.

show vpdn dead-cache {**group** *group-name* | **all** }

Syntax Description

group *group-name*	Displays all entries in the dead-cache for a specific virtual private dialup network (VPDN) group.
all	Displays 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.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.

Usage Guidelines

An LNS in a dead-cache cannot establish new sessions or calls. The VPDN dead-cache maintains a list of LNSs that have not responded to control messages or have sent a message indicating that a session was not created.

Use the **show vpdn dead-cache** command on the L2TP Access Concentrator (LAC) gateway to display a list of LNS entries in a dead-cache state. The list includes the IP address of the LNS, the VPDN session load, the status (DOWN, TESTABLE, and TESTING) of the LNS, and the time, in seconds, that the LNS entry has been in the specific dead-cache state.

You can configure the timeout for establishing new sessions or calls using the **l2tp tunnel busy timeout** command. The timeout starts when an LNS is added to the VPDN dead-cache. When the timeout expires, the LNS is available for the next session and timeout starts again.

The status of the LNS in the VPDN dead-cache changes from DOWN to TESTABLE when the timeout expires the first time. The status change from TESTABLE to TESTING when the first attempt is made to establish a session to the LNS. The status changes from TESTING to ACTIVE when a session successfully opened to the LNS or when the load is 0, and the LNS entry is removed from the VPDN dead-cache.

If the session fails to open to the LNS from any status, the status changes to DOWN and the timeout is restarted.

Use the **clear vpdn dead-cache** command on the LAC gateway to clear the list of LNS entries in the dead-cache. Once the LNS exits the dead-cache state, the LNS is active and can establish new sessions.

Use the **vpdn logging dead-cache** command in global configuration mode on the LAC gateway to trigger a system message log (syslog) event when an LNS enters or exits a dead-cache state.

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

Examples

The following sample output displays the status of the dead-cache for the specific VPDN group exampleA:

```
Router# show vpdn dead-cache group exampleA
```

```
vpdn-group ip address   load   status   changed time
exampleA   192.168.2.2  0      DOWN     00:01:58
```

The following example shows how to display the status of the dead-cache for all VPDN groups:

```
Router# show vpdn dead-cache all
```

```
vpdn-group  ip address    load   status   changed time
exampleA    192.168.2.2   0      DOWN     00:01:58
exampleB    192.168.2.3   7      TESTABLE 00:00:07
```

The table below describes the significant fields shown in the displays.

Table 15 show vpdn dead-cache Field Descriptions

Field	Description
vpdn-group	Assigned name of the VPDN group that is using the tunnel.
ip address	IP address of the LNS.
load	VPDN session load.
status	Status of the LNS.
changed time	Amount of time in hh:mm:ss the LNS has been in a dead-cache state.

Related Commands

Command	Description
clear vpdn dead-cache	Clears the entries in the dead-cache for VPDN groups.
l2tp tunnel busy timeout	Configures the time that the router waits before attempting to recontact an LNS that was previously busy.
vpdn logging dead-cache	Enables the logging of VPDN events.

show vpdn domain

To display all virtual private dialup network (VPDN) domains and DNIS groups configured on the network access server, use the **show vpdn domain** command in privileged EXEC mode.

show vpdn domain

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following is sample output from the **show vpdn domain** command:

```
Router# show vpdn domain
Tunnel             VPDN Group
------             ----------
dnis:cg2           vgdnis (L2F)
domain:twu-ultra   test (L2F)
```

The table below describes the significant fields shown in the display.

Table 16 show vpdn domain Field Descriptions

Field	Description
Tunnel	Assigned name of the tunnel endpoint.
VPDN Group	Assigned name of the VPDN group using the tunnel.

Related Commands

Command	Description
dnis (VPDN)	Specifies the DNIS group name or DNIS number of users that are to be forwarded to a tunnel server using a VPDN.
domain	Specifies the domain name of users that are to be forwarded to a tunnel server using a VPDN.

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

show vpdn group

To display group session-limit information on an Layer 2 Tunneling Protocol network server (LNS), use the **show vpdn group** command in privileged EXEC mode. When resource manager is enabled, to display a summary of the relationships among virtual private dialup network (VPDN) groups and customer/VPDN profiles, or to summarize the configuration of a VPDN group including DNIS/domain, load sharing information, and current session information, use the **show vpdn group** command in privileged EXEC mode.

show vpdn group [*name*] [**domain** | **endpoint**]

Syntax Description

name	(Optional) VPDN group name summarizes the configuration of the specified group.
domain	(Optional) DNIS/domain information.
endpoint	(Optional) Endpoint session information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(4)XI	This command was introduced.
12.2(8)T	The "resource-pool disabled" message was added to the command output.
12.2(33)XNE	The display was enhanced to show session-limit information on the LNS.
15.0(1)M	The display was enhanced to show session-limit information on the LNS.

Usage Guidelines

The following usage guidelines apply only to the Cisco AS5300, AS5400, and AS5800 access servers. If the resource manager is disabled by the **resource-pool disable** global configuration command, the **show vpdn group** command only displays a message stating that the resource-pool is disabled. If you enter the **show vpdn group** *name* command when the **resource-pool disable** command is enabled, the router displays the message stating that the resource-pool is disabled followed by a summary of active VPDN sessions.

If you enter the **show vpdn group** command without a group name, the display includes session-limit information for all groups on the LNS. If you enter the **show vpdn group** command with a group name, the display includes session-limit information for the specified group on the LNS. Session-limit information is not displayed on the L2TP access concentrator (LAC.)

Examples of the show vpdn group command output (with resource manager enabled)

The following is sample output from the **show vpdn group** command summarizing all VPDN group and profile relationships:

```
Router# show vpdn group
VPDN Group  Customer Profile  VPDN Profile
----------  ----------------  ------------
 1           -                 -
 2           -                 -
 3           -                 -
 lisun       cp1               -
 outgoing-2  -                 -
 test        -                 -
*vg1         cpdnis            -
*vg2         cpdnis            -
 vgdnis     +cp1               vp1
 vgnumber    -                 -
 vp1         -                 -
* VPDN group not configured
+ VPDN profile under Customer profile
```

Note A VPDN group is marked with "*" if it does not exist but is used under customer/VPDN profile.

Note Customer profiles are marked with "+" if the corresponding VPDN group is not directly configured under a customer profile. Instead, the corresponding VPDN profile is configured under the customer profile.

The following is sample output from the **show vpdn group** command for a VPDN group named vgdnis (when resource manager is enabled):

```
Router # show vpdn group vgdnis
Tunnel (L2TP)
------
dnis:cg1
dnis:cg2
dnis:jan
cisco.com
Endpoint        Session Limit Priority Active Sessions Status Reserved Sessions
--------        ------------- -------- --------------- ------ -----------------
172.21.9.67     *             1        0               OK     -
--------------- -------------          ---------------        -----------------
Total           *                      0                      0
```

Note Tunnel section lists all domain/DNIS ("dnis" appears before DNIS). The session limit endpoint is the sum of the session limits of all endpoints and is marked with "*" if there is no limit (indicated by "*") for any endpoint. If the endpoint has no session limit, reserved sessions are marked with "-".

The following is sample output from the **show vpdn group** command (when resource manager is configured):

```
Router# show vpdn group
VPDN Group      Customer Profile VPDN Profile
----------      ---------------- ------------
customer1-vpdng customer1        customer1-profile
customer2-vpdng customer2        -
Router# show vpdn group customer1-vpdng
Tunnel (L2TP)
--------
cisco.com
```

```
cisco1.com
dnis:customer1-calledg
Endpoint        Session Limit Priority Active Sessions Status Reserved Sessions
--------        ------------- -------- --------------- ------ -----------------
172.21.9.67     *             1        0               OK
172.21.9.68     100           1        0               OK
172.21.9.69     *             5        0               OK
                -------------          ---------------        -----------------
Total           *                      0                      0
```

The following is sample output from the **show vpdn group** command on a Cisco AS5300 access server when the **resource-pool disable** command is configured:

```
Router # show vpdn group
% Resource-pool disabled
```

The following is sample output from the **show vpdn group vpdnis** command on a Cisco AS5300 access server when the **resource-pool disable** command is configured. The summary of tunnel information is displayed only if there is an active VPDN session.

```
Router # show vpdn group vgdnis
% Resource-pool disabled
Tunnel (L2TP)
------
dnis:cg1
cisco.com
Endpoint        Session Limit Priority Active Sessions Status Reserved Sessions
--------        ------------- -------- --------------- ------ -----------------
172.21.9.67     *             1        1               OK     -
--------------  -------------          ---------------        -----------------
```

The table below describes the significant fields shown in the displays.

Table 17 show vpdn group Field Descriptions

Field	Description
VPDN Group	Assigned name of the VPDN group using the tunnel.
Customer Profile	Name of the assigned customer profile.
VPDN Profile	Name of the assigned VPDN profile.
Tunnel	Assigned name of the tunnel endpoint.
Endpoint	IP address of HGW/LNS router.
Session Limit	Number of sessions permitted for the designated endpoint.
Priority	Loadsharing HGW/LNSs are always marked with a priority of 1.
Active Sessions	Number of active sessions on the network access server. These are sessions successfully established with endpoints (not reserved sessions).
Status	Only two status types are possible: OK and busy.

Field	Description
Reserved Sessions	Authorized sessions that are waiting to see if they can successfully connect to endpoints. Essentially, these sessions are queued calls. In most cases, reserved sessions become active sessions.

Example of the show vpdn group command output for session-limit information on an LNS (with or without resource manager enabled)

The following is sample output from the **show vpdn group** command after configuring the client, the LAC, and the LNS, and after establishing sessions for two domains.

The **show vpdn group** command displays the group session-limit information only on the LNS (not on the LAC):

```
Router# show vpdn group
VPDN group vg1
Group session limit 65535  Active sessions 1  Active tunnels 1
VPDN group vg2
Group session limit 65535  Active sessions 1  Active tunnels 1
```

Related Commands

Command	Description
dnis (VPDN)	Specifies the DNIS group name or DNIS number of users that are to be forwarded to a tunnel server using a VPDN.
domain	Specifies the domain name of users that are to be forwarded to a tunnel server using a VPDN.
resource-pool profile customer	Creates a customer profile and enters customer profile configuration mode.
resource-pool profile vpdn	Creates a VPDN profile and enters VPDN profile configuration mode.
vpdn group	Associates a VPDN group with a customer or VPDN profile.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.

show vpdn group-select

To display a summary of the relationships among virtual private dialup network (VPDN) groups and customer or VPDN profiles, or to summarize the configuration of the default VPDN group including DNIS or domain, load sharing information, and current session information, use the **show vpdn group-select** command in user EXEC or in privileged EXEC mode.

show vpdn group-select {**summary** | **default**}

Syntax Description

summary	Displays details of a VPDN group.
default	Displays details of a default VPDN group.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

Use the **show vpdn group-select** command to see a summary of the relationships among VPDN groups and customer or VPDN profiles, or to summarize the configuration of the default VPDN group including domain or DNIS, load sharing information, and current session information.

Examples

The following is sample output from the **show vpdn group-select default** command summarizing all VPDN group and profile relationships:

```
Router> show vpdn group-select default
Default VPDN Group      Protocol
 vg                       l2tp
 None                     pptp
```

The following is sample output from the **show vpdn group-select summary** command:

```
Router> show vpdn group-select summary
VPDN Group      Vrf        Remote Name   Source-IP       Protocol Direction
 vg_ip2                                   0.0.0.0         l2tp     request-dialin
 vg_ip3                                   10.0.0.3        l2tp     request-dialin
 vg_lts1_ip2    lts1                      10.1.1.2        l2tp     accept-dialin
```

The table below describes the significant fields shown in the displays.

Table 18 show vpdn group-select Field Descriptions

Field	Description
VPDN Group	Assigned name of the VPDN group using the tunnel.
Vrf	Name of the VPN routing and forwarding (VFR) instance assigned.
Remote Name	Hostname of the remote peer.
Source-IP	Source IP address to which to map the destination IP addresses in subscriber traffic.
Protocol	Tunneling protocol that a VPDN subgroup will use.
Direction	Direction for dial requests for VPDN tunnels from a tunnel server.

Related Commands

Command	Description
source-ip	Specifies an IP address that is different from the physical IP address used to open a VPDN tunnel for the tunnels associated with a VPDN group.
terminate-from	Specifies the hostname of the remote LAC or LNS that is required when accepting a VPDN tunnel.
vpdn group	Associates a VPDN group with a customer or VPDN profile.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.
vpdn group-select keys	Displays a summary of the relationships among VPDN groups and customer or VPDN profiles, or to summarize the configuration of a VPDN group including DNIS or domain, load sharing information, and current session information based on a source IP address or VRF.
vpn	Specifies that the source and destination IP addresses of a given VPDN group belong to a specified VRF instance.

show vpdn group-select keys

To display a summary of the relationships among virtual private dialup network (VPDN) groups and customer or VPDN profiles, or to summarize the configuration of a VPDN group including DNIS or domain, load sharing information, and current session information, use the **show vpdn group-select keys** command in user EXEC or in privileged EXEC mode.

show vpdn group-select keys hostname *hostname* **source-ip** *ip-address* [**vpn** {**id** *vpn-id* | **vrf** *vrf-name*}]

Syntax Description

hostname *hostname*	Specifies the hostname of the user.
source-ip *ip-address*	Specifies the source IP address of the VPDN group.
vpn	(Optional) Specifies the VPDN group configurations based on the Virtual Private Network (VPN).
id *vpn-id*	(Optional) Specifies the VPDN group configurations based on the VPN ID.
vrf *vrf-name*	(Optional) Specifies the VPDN group configurations based on a virtual routing and forwarding (VRF) instance name.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Examples

The following is sample output from the **show vpdn group-select keys** command for a host with the name lac-1 and an IP address of 10.0.0.1:

```
Router# show vpdn group-select keys vrf vrf-blue hostname lac-1 source-ip 10.0.0.1
VPDN Group       Vrf        Hostname   Source Ip
vg1              vrf-blue   lac-1      10.0.0.1
```

The following is sample output from the **show vpdn group-select keys** command for a host with the name lac-5 and an IP address of 10.1.1.0, and VRF name vrf-red:

```
Router# show vpdn group-select keys vrf vrf-red hostname lac-5 source-ip 10.1.1.0
```

```
VPDN Group    Vrf        Hostname    Source Ip
Vg2           vrf-red    lac-5         10.1.1.0
```

Related Commands

Command	Description
source-ip	Specifies an IP address that is different from the physical IP address used to open a VPDN tunnel for the tunnels associated with a VPDN group.
terminate-from	Specifies the hostname of the remote LAC or LNS that will be required when accepting a VPDN tunnel.
vpdn group	Associates a VPDN group with a customer or VPDN profile.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.
vpdn group-select	Display a summary of the relationships among VPDN groups and customer or VPDN profiles, or to summarize the configuration of the default VPDN group including DNIS or domain, load sharing information, and current session information.
vpn	Specifies that the source and destination IP addresses of a given VPDN group belong to a specified VRF instance.

show vpdn history failure

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

show vpdn history failure [*user-name*]

Syntax Description

user-name	(Optional) Username, which displays only the entries mapped to that particular user.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

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

You can obtain failure results for the output of the **show vpdn history failure** command by referencing RFC 2661, Section 4.4.2, L2TP Result and Error Codes.

Examples

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

```
Router# show vpdn history failure
Table size: 20
Number of entries in table: 1
User: example@example.com, MID = 1
NAS: isp, IP address = 172.21.9.25, CLID = 1
Gateway: hp-gw, IP address = 172.21.9.15, CLID = 1
Log time: 13:08:02, Error repeat count: 1
Failure type: The remote server closed this session
Failure reason: Administrative intervention
```

The table below describes the significant fields shown in the display.

Table 19 show vpdn history failure Field Descriptions

Field	Description
Table size	Configurable VPDN history table size.

Field	Description
Number of entries in table	Number of entries currently in the history table.
User	Username for the entry displayed.
MID	VPDN user session ID that correlates to the logged event. The MID is a unique ID per user session.
NAS	Network access server identity.
IP address	IP address of the network access server or home gateway (HGW).
CLID	Tunnel endpoint for the network access server and HGW.
Gateway	HGW end of the VPDN tunnel.
Log time	Event logged time.
Error repeat count	Number of times a failure entry has been logged under a specific user. Only one log entry is allowed per user and is unique to its MID, with the older one being overwritten.
Failure type	Description of failure.
Failure reason	Reason for failure. **Note** To determine failure reasons, refer to RFC 2661, Section 4.4.2.

Related Commands

Command	Description
clear vpdn history failure	Clears the content of the VPDN failure history table.
vpdn history failure	Enables logging of VPDN failures to the history failure table or to sets the failure history table size.

show vpdn multilink

To display the multilink sessions authorized for all virtual private dialup network (VPDN) groups, use the **show vpdn multilink** command in privileged EXEC mode.

show vpdn multilink

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following is sample output comparing the **show vpdn tunnel** command with the **show vpdn multilink** command:

```
Router# show vpdn tunnel
L2F Tunnel and Session Information (Total tunnels=1 sessions=1)
 NAS CLID HGW CLID NAS Name        HGW Name        State
 24       10       centi3_nas      twu253_hg       open
                   172.21.9.46     172.21.9.67
 CLID   MID    Username                  Intf   State
 10     1      twu@twu-ultra.cisco.com    Se0:22 open
Router# show vpdn multilink
Multilink Bundle Name   VPDN Group Active links Reserved links Bundle/Link Limit
---------------------   ---------- ------------ -------------- -----------------
twu@twu-ultra.cisco.com vgdnis     1            0              */*
```

The table below describes the significant fields shown in the display.

Table 20 show vpdn multilink Field Descriptions

Field	Description
NAS CLID	Network access server Caller Line Identification number (CLID).
HGW CLID	Home gateway (HGW) Caller Line Identification number (CLID).
NAS Name	Name assigned to the NAS.

Field	Description
HGW Name	Name assigned to the HGW.
State	Operational state of the designated piece of equipment.
CLID	Calling Line Identification number.
MID	Modem Identification.
Username	Assigned user name.
Intf	Type of interface.
State	Operational state of the designated piece of equipment.
Multilink Bundle Name	Name of the multilink bundle.
VPDN Group	Name of the VPDN group.
Active Links	Number of active links.
Reserved Links	Number of reserved links.
Bundle/Link limit	Limit of bundles or links available.

Related Commands

Command	Description
multilink	Limits the total number MLP sessions for all VPDN multilink users.

show vpdn redirect

To display statistics for Layer 2 Tunneling Protocol (L2TP) redirects and forwards, use the **show vpdn redirect** command in privileged EXEC mode.

show 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

Statistics about the number of L2TP forwards and redirects that were done by the router as an L2TP network access server (NAS) or L2TP tunnel server are displayed when you enter the **show vpdn redirect** command. To clear the redirect counters, use the **clear vpdn redirect** command.

Examples

The following example displays statistics for redirects and forwards for a router configured as an L2TP NAS:

```
Router# show vpdn redirect
vpdn redirection enabled
sessions redirected as access concentrator: 2
sessions redirected as network server: 0
sessions forwarded: 2
```

The table below describes the significant fields shown in the display.

Table 21 show vpdn redirect Field Descriptions

Field	Description
vpdn redirection enabled	Verifies that L2TP redirect is enabled.

Field	Description
sessions redirected as access concentrator	Displays the number of sessions that the router has redirected when configured as a NAS.
sessions redirected as network server	Displays the number of sessions that the router has redirected when configured as a tunnel server.
sessions forwarded	Displays the total number of sessions that have been forwarded.

Related Commands

Command	Description
clear vpdn redirect	Clears the L2TP redirect counters shown in the output from the **show vpdn redirect** command.
vpdn redirect	Enables L2TP redirect functionality.
vpdn redirect attempts	Restricts the number of redirect attempts possible for an L2TP call on the NAS.
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.

show vpdn redundancy

To display information about the state of the virtual private dialup network (VPDN), use the **show vpdn redundancy** command in user EXEC or in privileged EXEC mode.

show vpdn redundancy [**all** | [**detail**] [**id** *local-tunnel-ID* [*local-session-ID*]]]

Syntax Description

all	(Optional) Displays a summary of all VPDN redundancy data.
detail	(Optional) Displays detailed information about L2TP redundancy.
id	(Optional) Displays redundancy information about the specified local tunnel or local session.
local-tunnel-ID	(Optional) Displays redundancy information about the specified local session. The range is 1 to 4294967295.
local-session-ID	(Optional) Displays redundancy information about the specified local tunnel. The range is 1 to 4294967295.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.2.	This command was introduced.
Cisco IOS XE Release 3.3S	This command was modified. The**show vpdn redundancy detail** command output was enhanced to provide counters for tunnels and sessions cleared during the resynchronization phase. The**show vpdn redundancy** command output was enhanced to show whether the resynchronization has started or not started.

Usage Guidelines

Use the **show vpdn redundancy all** command to display the status of VPDN redundancy information.

The **show vpdn redundancy** command displays the same information as the **show l2tp redundancy** command.

During the time frame immediately after a switchover and before the resynchronization starts, if you enter the **show l2tp redundancy** command, the last line of the command output is "Resync not yet started." Once the resynchronization starts, the line "L2TP Resynced Tunnels: 0/0 (success/fail)" is shown. When the resynchronization completes, the "Resync duration 0.0 secs (complete)" is shown.

Examples

The following example shows how to display the status of VPDN redundancy information:

```
Router# show vpdn redundancy
L2TP HA support: Silent Failover
L2TP HA Status:
  Checkpoint Messaging on: TRUE
  Standby RP is up:        TRUE
  Recv'd Message Count:    189
  L2TP Tunnels:            2/2/2/0 (total/HA-enabled/HA-est/resync)
  L2TP Sessions:           20/20/20 (total/HA-enabled/HA-est)
  L2TP Resynced Tunnels:   2/0 (success/fail)
  Resync duration 0.63 secs (complete)
```

The following example shows how to display the global status of all VPDN redundancy information:

```
Router# show vpdn redundancy all
L2TP HA support: Silent Failover
L2TP HA Status:
 Checkpoint Messaging on:                            FALSE
 Standby RP is up:                            TRUE
 Recv’d Message Count:                            0
 L2TP Active Tunnels:                            1/1 (total/HA-enable)
 L2TP Active Sessions:                            2/2 (total/HA-enable)
L2TP HA CC Check Point Status:
State            LocID        RemID        Remote Name                Class/
Group                            Num/Sessions
est            44233        51773        LNS                VPDN Group 1
10.1.1.1                            2
L2TP HA Session Status:
LocID        RemID        TunID            Waiting for                    Waiting for
                            VPDN app?                    L2TP proto?
2        2        44233            No                    No
2        3        44233            No                    No
```

The following example shows how to limit the displayed redundancy information to only the sessions associated with a specified tunnel ID:

```
Router# show vpdn redundancy id 44233
L2TP HA Session Status:
LocID        RemID        TunID            Waiting for                    Waiting for
                            VPDN app?                    L2TP proto?
2        2        44233            No                    No
2        3        44233            No                    No
```

The table below describes the significant fields shown in the **show vpdn redundancy**, **show vpdn redundancy all**, **show vpdn redundancy id**, and in the **show vpdn redundancy detail** command outputs.

Table 22 show vpdn redundancy Command Field Descriptions

Field	Description
Checkpoint Messaging on	Operational status of the checkpoint messaging infrastructure.
Standby RP is up	Operational status of the standby Route Processor (RP).

Field	Description
Recv’d Message Count	Number of checkpoint messages received on this RP.
L2TP Tunnels	Operational status of L2TP HA tunnels: • total--Number of L2TP tunnels operating on this router. • HA-enabled--Number of L2TP tunnels currently configured to be checkpointed to the standby RP. • HA-est--Number of HA tunnels currently established (as opposed to configured). • resync--Number of tunnels currently being resynchronized (usually during a switchover event).
L2TP Sessions	Operational status of L2TP HA sessions: • total--Number of L2TP sessions operating on this router. • HA-enabled--Number of L2TP sessions currently configured to be checkpointed to the standby RP. • HA-est--Number of HA sessions currently established (as opposed to configured).
L2TP Resynced Tunnels	Number of successful and failed L2TP resynchronized tunnels.
Resync duration	How long the resynchronization took, in seconds.
L2TP HA CC Check Point Status	
State	Status of the tunnel.
LocID	Local ID of the L2TP HA tunnel.
RemID	Remote tunnel ID.
Remote Name	Router name associated with this tunnel.
Class/Group	Unique number associated with the class or group as defined in the L2TP or VPDN configuration.
Num/Sessions	Number of sessions currently set up over the tunnel or CC.
Waiting for VPDN app	Status of the virtual private dialup network (VPDN) application checkpointing delay. The VPDN application checkpointing could delay the completion of the session setup.

Field	Description
Waiting for L2TP proto	Status of the L2TP protocol checkpointing delay. The L2TP protocol checkpointing could delay the completion of the session setup.
Tunnels destroyed during tunnel resync phase	
Poisoned	Number of L2TP tunnels poisoned during the resynchronization phase.
Failed to transmit the initial probe	Number of L2TP tunnels where the initial probe packet could not be transmitted during the resynchronization phase.
Cleared by peer	Number of L2TP tunnels cleared by the peer during the resynchronization phase.
Cleared due to excessive retransmits	Number of L2TP tunnels cleared due to an excessive number of probe retransmissions during the resynchronization phase.
Cleared because unestablished	Number of L2TP tunnels cleared because they not completely established at the start of the resynchronization phase.
Cleared by us, other	Number of L2TP tunnels cleared for other reasons during the resynchronization phase.
Total	Total number of tunnels destroyed during the resynchronization phase.
Sessions destroyed during tunnel resync phase	
Poisoned	Number of L2TP sessions poisoned during the resynchronization phase.
Unestablished	Number of L2TP sessions cleared because they not completely established at the start of the resynchronization phase.
Missing application session	Number of L2TP sessions cleared because no corresponding VPDN session is at the end of the resynchronization phase.
Cleared by peer	Number of L2TP sessions cleared by the peer during the resynchronization phase.
Attempted before or during resync	Number of L2TP sessions attempted by the peer (after failover) before or during the resynchronization phase.

Field	Description
Tunnel poisoned	Number of L2TP sessions cleared because the tunnel carrying them was poisoned during the resynchronization phase.
Tunnel failed to transmit initial probe	Number of L2TP sessions cleared because the initial probe packet could not be transmitted on the tunnel.
Tunnel cleared by peer	Number of L2TP sessions cleared because the tunnel carrying them was cleared by the peer.
Tunnel cleared due to excessive retransmits	Number of L2TP sessions cleared because of an excessive number of retransmissions on the tunnel carrying them.
Tunnel cleared because unestablished	Number of L2TP sessions cleared because the tunnel carrying them was not completely established at the start of the resynchronization phase.
Tunnel cleared by us, other	Number of L2TP sessions cleared because the tunnel carrying them was cleared for some reason.
Sessions cleared, other	Number of sessions cleared for other reasons during the resynchronization phase.
Total	Total number of sessions destroyed during the resynchronization phase.

The following example shows how to limit the information displayed by providing a tunnel ID:

```
Router# show vpdn redundancy id 44233
 L2TP HA Session Status:
LocID        RemID        TunID            Waiting for                    Waiting for
                            VPDN app?                    L2TP proto?
2        2        44233            No                    No
```

The following example shows how to limit the information displayed by providing a session ID:

```
Router# show vpdn redundancy detail id 44233 3
 Local session ID                                : 2
 Remote session ID                                : 2
 Local CC ID                                : 44233
 Local UDP port                                : 1701
 Remote UDP port                                : 1701
 Waiting for VPDN application                                : No
 Waiting for L2TP protocol                                : No
```

The following example shows the detailed information displayed on a router newly active after a failover:

```
Router# show vpdn redundancy detail
L2TP HA Status:
  Checkpoint Messaging on: TRUE
  Standby RP is up:        TRUE
  Recv'd Message Count:    219
  L2TP Tunnels:            1/1/1/0 (total/HA-enabled/HA-est/resync)
  L2TP Sessions:           1/1/1 (total/HA-enabled/HA-est)
  L2TP Resynced Tunnels:   1/0 (success/fail)
  Resync duration 3.0 secs (complete)
```

```
Our Ns checkpoints: 0, our Nr checkpoints: 0
Peer Ns checkpoints: 0, peer Nr checkpoints: 0
Packets received before entering resync phase: 0
Nr0 adjusts during resync phase init: 0
Nr learnt from peer during resync phase: 0
Tunnels destroyed during tunnel resync phase
  Poisoned:                                 1
  Failed to transmit the initial probe:     2
  Cleared by peer:                          3
  Cleared due to excessive retransmits:     4
  Cleared because unestablished:            5
  Cleared by us, other:                     6
Total:                                     21
Sessions destroyed during tunnel resync phase
  Poisoned:                                       7
  Unestablished:                                  8
  Missing application session:                    9
  Cleared by peer:                               10
  Attempted before or during resync:             11
  Tunnel poisoned:                               12
  Tunnel failed to transmit initial probe:       13
  Tunnel cleared by peer:                        14
  Tunnel cleared due to excessive retransmits:   15
  Tunnel cleared because unestablished:          16
  Tunnel cleared by us, other:                   17
  Sessions cleared, other:                       18
Total:                                          134
```

Related Commands

Command	Description
debug l2tp redundancy	Displays information on L2TP sessions having checkpoint events and errors.
debug vpdn redundancy	Displays information on VPDN sessions having checkpoint events and errors.
l2tp sso enable	Enables L2TP HA.
l2tp tunnel resync	Specifies the number of packets sent before waiting for an acknowledgment message.
show l2tp redundancy	Displays L2TP sessions containing redundancy data.
sso enable	Enables L2TP HA for VPDN groups.

show vpdn session

To display session information about active Layer 2 sessions for a virtual private dialup network (VPDN), use the **show vpdn session** command in privileged EXEC mode.

show vpdn session [**l2f** | **l2tp** | **pptp**] [**all** | **packets** [**ipv6**] | **sequence** | **state** [*filter*]]

Syntax Description

l2f	(Optional) Displays information about Layer 2 Forwarding (L2F) calls only.
l2tp	(Optional) Displays information about Layer 2 Tunneling Protocol (L2TP) calls only.
pptp	(Optional) Displays information about Point-to-Point Tunnel Protocol (PPTP) calls only.
all	(Optional) Displays extensive reports about active sessions.
packets	(Optional) Displays information about packet and byte counts for sessions.
ipv6	(Optional) Displays IPv6 packet and byte-count statistics.
sequence	(Optional) Displays sequence information for sessions.
state	(Optional) Displays state information for sessions.
filter	(Optional) One of the filter parameters defined in the table below.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.2	This command was introduced.
12.1(1)T	This command was enhanced to display Point-to-Point Protocol over Ethernet (PPPoE) session information. The **packets** and **all** keywords were added.

Release	Modification
12.1(2)T	This command was enhanced to display PPPoE session information on actual Ethernet interfaces.
12.2(13)T	Reports from this command were enhanced with a unique identifier that can be used to correlate a particular session with the session information retrieved from other **show** commands or **debug** command traces.
12.3(2)T	The **l2f**, **l2tp**, and the **pptp** keywords were added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.4(11)T	The **l2f** keyword was removed.
Cisco IOS XE Release 2.5	This command was implemented on Cisco ASR 1000 series routers.
Cisco IOS XE Release 2.6	The **ipv6** keyword was added. The **show vpdn session** command with the **all** and the **l2tp all** keywords was modified to display IPv6 counter information.

Usage Guidelines

Use the **show vpdn session** command to display information about all active sessions using L2TP, L2F, and PPTP.

The output of the **show vpdn session** command displays PPPoE session information as well. PPPoE is supported on ATM permanent virtual connections (PVCs) compliant with RFC 1483 only. PPPoE is not supported on Frame Relay and any other LAN interfaces such as FDDI and Token Ring.

Reports and options for this command depend upon the configuration in which it is used. Use the command-line question mark (?) help function to display options available with the **show vpdn session** command.

The table below defines the filter parameters available to refine the output of the **show vpdn session** command. You can use any one of the filter parameters in place of the *filter* argument.

Table 23 Filter Parameters for the show vpdn session Command

Syntax	Description
interface serial *number*	Filters the output to display only information for sessions associated with the specified serial interface. • *number* --The serial interface number.

Syntax	Description
interface virtual-template *number*	Filters the output to display only information for sessions associated with the specified virtual template. • *number* --The virtual template number.
tunnel id *tunnel-id session-id*	Filters the output to display only information for sessions associated with the specified tunnel ID and session ID. • *tunnel-id* --The local tunnel ID. The range is 1 to 65535. • *session-id* --The local session ID. The range is 1 to 65535.
tunnel remote-name *remote-name local-name*	Filters the output to display only information for sessions associated with the tunnel with the specified names. • *remote-name* --The remote tunnel name. • *local-name* --The local tunnel name.
username *username*	Filters the output to display only information for sessions associated with the specified username. • *username* --The username.

The **show vpdn session** command provides reports on call activity for all active sessions. The following output is from a device carrying active L2TP, L2F, and PPPoE sessions:

```
Router# show vpdn session
L2TP Session Information Total tunnels 1 sessions 4
LocID RemID TunID Intf          Username             State    Last Chg Uniq ID
4     691   13695 Se0/0         nobody2@cisco.com        est    00:06:00  4
5     692   13695 SSS Circuit   nobody1@cisco.com        est    00:01:43  8
6     693   13695 SSS Circuit   nobody1@cisco.com        est    00:01:43  9
3     690   13695 SSS Circuit   nobody3@cisco.com        est    2d21h     3
L2F Session Information Total tunnels 1 sessions 2
 CLID   MID    Username                   Intf          State   Uniq ID
 1      2      nobody@cisco.com              SSS Circuit   open    10
 1      3      nobody@cisco.com              SSS Circuit   open    11
%No active PPTP tunnels
PPPoE Session Information Total tunnels 1 sessions 7
PPPoE Session Information
UID    SID    RemMAC         OIntf          Intf      Session
              LocMAC                        VASt      state
3      1      0030.949b.b4a0 Fa2/0          N/A       CNCT_FWDED
              0010.7b90.0840
6      2      0030.949b.b4a0 Fa2/0          Vi1.1     CNCT_PTA
              0010.7b90.0840               UP
7      3      0030.949b.b4a0 Fa2/0          Vi1.2     CNCT_PTA
              0010.7b90.0840               UP
8      4      0030.949b.b4a0 Fa2/0          N/A       CNCT_FWDED
              0010.7b90.0840
9      5      0030.949b.b4a0 Fa2/0          N/A       CNCT_FWDED
              0010.7b90.0840
10     6      0030.949b.b4a0 Fa2/0          N/A       CNCT_FWDED
              0010.7b90.0840
11     7      0030.949b.b4a0 Fa2/0          N/A       CNCT_FWDED
              0010.7b90.0840
```

The table below describes the significant fields shown in the **show vpdn session** display.

Table 24 show vpdn session Field Descriptions

Field	Description
LocID	Local identifier.
RemID	Remote identifier.
TunID	Tunnel identifier.
Intf	Interface associated with the session.
Username	User domain name.
State	Status for the individual user in the tunnel; can be one of the following states: • est • opening • open • closing • closed • waiting_for_tunnel The waiting_for_tunnel state means that the user connection is waiting until the main tunnel can be brought up before it moves to the opening state.
Last Chg	Time interval (in hh:mm:ss) since the last change occurred.
Uniq ID	The unique identifier used to correlate this particular session with the sessions retrieved from other **show** commands or **debug** command traces.
CLID	Number uniquely identifying the session.
MID	Number uniquely identifying this user in this tunnel.
UID	PPPoE user ID.
SID	PPPoE session ID.
RemMAC	Remote MAC address of the host.
LocMAC	Local MAC address of the router. It is the default MAC address of the router.
OIntf	Outgoing interface.
Intf VASt	Virtual access interface number and state.

Field	Description
Session state	PPPoE session state.

The **show vpdn session packets** command provides reports on call activity for all the currently active sessions. The following output is from a device carrying an active PPPoE session:

```
Router# show vpdn session packets

%No active L2TP tunnels
%No active L2F tunnels

PPPoE Session Information Total tunnels 1 sessions 1
PPPoE Session Information
SID     Pkts-In         Pkts-Out        Bytes-In        Bytes-Out
1       202333          202337          2832652         2832716
```

The table below describes the significant fields shown in the **show vpdn session packets** command display.

Table 25 show vpdn session packets Field Descriptions

Field	Description
SID	Session ID for the PPPoE session.
Pkts-In	Number of packets coming into this session.
Pkts-Out	Number of packets going out of this session.
Bytes-In	Number of bytes coming into this session.
Bytes-Out	Number of bytes going out of this session.

The **show vpdn session all** command provides extensive reports on call activity for all the currently active sessions. The following output is from a device carrying active L2TP, L2F, and PPPoE sessions:

```
Router# show vpdn session all
L2TP Session Information Total tunnels 1 sessions 4
Session id 5 is up, tunnel id 13695
Call serial number is 3355500002
Remote tunnel name is User03
  Internet address is 10.0.0.63
  Session state is established, time since change 00:03:53
    52 Packets sent, 52 received
    2080 Bytes sent, 1316 received
  Last clearing of "show vpdn" counters never
  Session MTU is 1464 bytes
  Session username is nobody@cisco.com
    Interface
    Remote session id is 692, remote tunnel id 58582
  UDP checksums are disabled
  SSS switching enabled
  No FS cached header information available
  Sequencing is off
  Unique ID is 8
Session id 6 is up, tunnel id 13695
Call serial number is 3355500003
Remote tunnel name is User03
  Internet address is 10.0.0.63
  Session state is established, time since change 00:04:22
    52 Packets sent, 52 received
    2080 Bytes sent, 1316 received
  Last clearing of "show vpdn" counters never
```

```
    Session MTU is 1464 bytes
    Session username is nobody@cisco.com
      Interface
      Remote session id is 693, remote tunnel id 58582
    UDP checksums are disabled
    SSS switching enabled
    No FS cached header information available
    Sequencing is off
    Unique ID is 9
  Session id 3 is up, tunnel id 13695
  Call serial number is 3355500000
  Remote tunnel name is User03
    Internet address is 10.0.0.63
    Session state is established, time since change 2d21h
      48693 Packets sent, 48692 received
      1947720 Bytes sent, 1314568 received
    Last clearing of "show vpdn" counters never
    Session MTU is 1464 bytes
    Session username is nobody2@cisco.com
      Interface
      Remote session id is 690, remote tunnel id 58582
    UDP checksums are disabled
    SSS switching enabled
    No FS cached header information available
    Sequencing is off
    Unique ID is 3
  Session id 4 is up, tunnel id 13695
  Call serial number is 3355500001
  Remote tunnel name is User03
    Internet address is 10.0.0.63
    Session state is established, time since change 00:08:40
      109 Packets sent, 3 received
      1756 Bytes sent, 54 received
    Last clearing of "show vpdn" counters never
    Session MTU is 1464 bytes
    Session username is nobody@cisco.com
      Interface Se0/0
      Remote session id is 691, remote tunnel id 58582
    UDP checksums are disabled
    IDB switching enabled
    FS cached header information:
      encap size = 36 bytes
      4500001C BDDC0000 FF11E977 0A00003E
      0A00003F 06A506A5 00080000 0202E4D6
      02B30000
    Sequencing is off
    Unique ID is 4
  L2F Session Information Total tunnels 1 sessions 2
  MID: 2
  User:  nobody@cisco.com
  Interface:
  State:  open
  Packets out: 53
  Bytes out: 2264
  Packets in: 51
  Bytes in: 1274
  Unique ID: 10
    Last clearing of "show vpdn" counters never
  MID: 3
  User:  nobody@cisco.com
  Interface:
  State:  open
  Packets out: 53
  Bytes out: 2264
  Packets in: 51
  Bytes in: 1274
  Unique ID: 11

  Last clearing of "show vpdn" counters never
  %No active PPTP tunnels
  PPPoE Session Information Total tunnels 1 sessions 7
  PPPoE Session Information
  SID     Pkts-In         Pkts-Out        Bytes-In        Bytes-Out
```

```
1       48696           48696           681765          1314657
2       71              73              1019            1043
3       71              73              1019            1043
4       61              62              879             1567
5       61              62              879             1567
6       55              55              791             1363
7       55              55              795             1363
```

The significant fields shown in the **show vpdn session all** command display are similar to those defined in the show vpdn session packets Field Descriptions and the show vpdn session Field Descriptions tables above.

Related Commands

Command	Description
show sss session	Displays Subscriber Service Switch session status.
show vpdn	Displays basic information about all active VPDN tunnels.
show vpdn domain	Displays all VPDN domains and DNIS groups configured on the NAS.
show vpdn group	Displays a summary of the relationships among VPDN groups and customer/VPDN profiles, or summarizes the configuration of a VPDN group including DNIS/domain, load sharing information, and current session information.
show vpdn history failure	Displays the content of the failure history table.
show vpdn multilink	Displays the multilink sessions authorized for all VPDN groups.
show vpdn redirect	Displays statistics for L2TP redirects and forwards.
show vpdn tunnel	Displays information about active Layer 2 tunnels for a VPDN.

show vpdn tunnel

To display information about active Layer 2 tunnels for a virtual private dialup network (VPDN), use the **show vpdn tunnel** command in privileged EXEC mode.

show vpdn tunnel [**l2f** | **l2tp** | **pptp**] [**all** [*filter*] | **packets** [**ipv6**] [*filter*] | **state** [*filter*] | **summary** [*filter*] | **transport** [*filter*]]

Syntax Description

l2f	(Optional) Specifies that only information about Layer 2 Forwarding (L2F) tunnels will be displayed.
l2tp	(Optional) Specifies that only information about Layer 2 Tunneling Protocol (L2TP) tunnels will be displayed.
pptp	(Optional) Specifies that only information about Point-to-Point Tunnel Protocol (PPTP) tunnels will be displayed.
all	(Optional) Displays summary information about all active tunnels.
filter	(Optional) One of the filter parameters defined in the Filter Parameters for the show vpdn tunnel Command table.
packets	(Optional) Displays packet numbers and packet byte information.
ipv6	(Optional) Displays IPv6 packet and byte-count statistics.
state	(Optional) Displays state information for a tunnel.
summary	(Optional) Displays a summary of tunnel information.
transport	(Optional) Displays tunnel transport information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.2	This command was introduced.

Release	Modification
12.1(1)T	The **packets** and **all** keywords were added.
12.3(2)T	The**l2f**, **l2tp**, and the **pptp** keywords were added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and support was added for L2TP congestion avoidance statistics.
12.4(11)T	The **l2f** keyword was removed.
12.2(33)SB	This command's output was modified and implemented on the Cisco 10000 series router for the PRE3 and PRE4 as described in the Usage Guidelines.
Cisco IOS XE Release 2.6	The **ipv6** keyword was added. The **show vpdn tunnel** command with the **all** and the **l2tp all** keywords was modified to display IPv6 counter information.

Usage Guidelines

Use the **show vpdn tunnel** command to display detailed information about L2TP, L2F, and PPTP VPDN tunnels.

The table below defines the filter parameters available to refine the output of the **show vpdn tunnel** command. You can use any one of the filter parameters in place of the *filter* argument.

Table 26 Filter Parameters for the show vpdn tunnel Command

Syntax	Description
id *local-id*	Filters the output to display only information for the tunnel with the specified local ID. • *local-id* --The local tunnel ID number. The range is 1 to 65535.
local-name *local-name remote-name*	Filters the output to display only information for the tunnel associated with the specified names. • *local-name* --The local tunnel name. • *remote-name* --The remote tunnel name.
remote-name *remote-name local-name*	Filters the output to display only information for the tunnel associated with the specified names. • *remote-name* --The remote tunnel name. • *local-name* --The local tunnel name.

Cisco 10000 Series Router Usage Guidelines

In Cisco IOS Release 12.2(33)SB, the **show vpdn tunnel summary** command no longer displays the active PPPoE sessions. Instead, use the **show pppoe sessions** command to display the active sessions.

In Cisco IOS Release 12.2(31)SB, the **show vpdn tunnel summary** command does display the active PPPoE sessions.

Examples

The following is sample output from the **show vpdn tunnel** command for L2F and L2TP sessions:

```
Router# show vpdn tunnel

L2TP Tunnel Information (Total tunnels=1 sessions=1)
LocID RemID Remote Name   State  Remote Address  Port  Sessions
2     10    router1       est    172.21.9.13     1701  1
L2F Tunnel
 NAS CLID HGW CLID NAS Name        HGW Name        State
 9        1        nas1            HGW1            open
                   172.21.9.4       172.21.9.232
%No active PPTP tunnels
```

The table below describes the significant fields shown in the display.

Table 27 show vpdn tunnel Field Descriptions

Field	Description
LocID	Local tunnel identifier.
RemID	Remote tunnel identifier.
Remote Name	Hostname of the remote peer.
State	Status for the individual user in the tunnel; can be one of the following states: • est • opening • open • closing • closed • waiting_for_tunnel The waiting_for_tunnel state means that the user connection is waiting until the main tunnel can be brought up before it moves to the opening state.
Remote address	IP address of the remote peer.
Port	Port ID.
Sessions	Number of sessions using the tunnel.
NAS CLID	Number uniquely identifying the VPDN tunnel on the network access server (NAS).

Field	Description
HGW CLID	Number uniquely identifying the VPDN tunnel on the gateway.
NAS Name	Hostname and IP address of the NAS.
HGW Name	Hostname and IP address of the home gateway.

The following example shows L2TP tunnel activity, including information about the L2TP congestion avoidance:

```
Router# show vpdn tunnel l2tp all
L2TP Tunnel Information Total tunnels 1 sessions 1
Tunnel id 30597 is up, remote id is 45078, 1 active sessions
  Tunnel state is established, time since change 00:08:27
  Tunnel transport is UDP (17)
  Remote tunnel name is LAC1
    Internet Address 172.18.184.230, port 1701
  Local tunnel name is LNS1
    Internet Address 172.18.184.231, port 1701
  Tunnel domain unknown
  VPDN group for tunnel is 1
  L2TP class for tunnel is
  4 packets sent, 3 received
  194 bytes sent, 42 received
  Last clearing of "show vpdn" counters never
  Control Ns 2, Nr 4
  Local RWS 1024 (default), Remote RWS 256
  In Use Remote RWS 15
  Control channel Congestion Control is enabled
    Congestion Window size, Cwnd 3
    Slow Start threshold, Ssthresh 256
    Mode of operation is Slow Start
  Tunnel PMTU checking disabled
  Retransmission time 1, max 2 seconds
  Unsent queuesize 0, max 0
  Resend queuesize 0, max 1
  Total resends 0, ZLB ACKs sent 2
  Current nosession queue check 0 of 5
  Retransmit time distribution: 0 0 0 0 0 0 0 0 0
  Sessions disconnected due to lack of resources 0
  Control message authentication is disabled
```

The table below describes the significant fields shown in the display.

Table 28 show vpdn tunnel all Field Descriptions

Field	Description
Local RWS	Size of the locally configured receive window.
Remote RWS	Size of the receive window advertised by the remote peer.
In Use RWS	Actual size of the receive window, if that value differs from the value advertised by the remote peer.
Congestion Window size, Cwnd 3	Current size of the congestion window (Cwnd).
Slow Start threshold, Ssthresh 500	Current value of the slow start threshold (Ssthresh).

Field	Description
Mode of operation is...	Indicates if the router is operating in Slow Start or Congestion Avoidance mode.

Related Commands

Command	Description
show vpdn	Displays basic information about all active VPDN tunnels.
show vpdn domain	Displays all VPDN domains and DNIS groups configured on the NAS.
show vpdn group	Displays a summary of the relationships among VPDN groups and customer/VPDN profiles, or summarizes the configuration of a VPDN group including DNIS/domain, load sharing information, and current session information.
show vpdn history failure	Displays the content of the failure history table.
show vpdn multilink	Displays the multilink sessions authorized for all VPDN groups.
show vpdn redirect	Displays statistics for L2TP redirects and forwards.
show vpdn session	Displays session information about active Layer 2 sessions for a VPDN.

show vtemplate

To display information about all configured virtual templates, use the **show vtemplate** command in privileged EXEC mode.

show vtemplate

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(7)DC	This command was introduced on the Cisco 6400 NRP.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3(14)T	The show display was modified to display the interface type of the virtual template and to provide counters on a per-interface-type basis for IPsec virtual tunnel interfaces.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Examples

The following is sample output from the **show vtemplate** command:

```
Router# show vtemplate
Virtual access subinterface creation is globally enabled
         Active     Active    Subint  Pre-clone Pre-clone Interface
       Interface Subinterface Capable Available   Limit     Type
       --------- ------------ ------- --------- --------- ---------
Vt1            0            0   Yes          --        --   Serial
Vt2            0            0   Yes          --        --   Serial
Vt4            0            0   Yes          --        --   Serial
Vt21           0            0    No          --        --   Tunnel
Vt22           0            0   Yes          --        --   Ether
Vt23           0            0   Yes          --        --   Serial
Vt24           0            0   Yes          --        --   Serial
Usage Summary
                              Interface   Subinterface
                              ---------   ------------
Current Serial  in use                1              0
Current Serial  free                0            3
Current Ether   in use              0            0
Current Ether   free                0            0
Current Tunnel  in use              0            0
Current Tunnel  free                0            0
Total                               1            3
Cumulative created                  8            4
Cumulative freed                    0            4
Base virtual access interfaces: 1
Total create or clone requests: 0
Current request queue size: 0
Current free pending: 0
Maximum request duration: 0 msec
Average request duration: 0 msec
Last request duration: 0 msec
Maximum processing duration: 0 msec
Average processing duration: 0 msec
Last processing duration: 0 msec
Last processing duration:0 msec
```

The table below describes the significant fields shown in the example.

Table 29 show vtemplate Field Descriptions

Field	Description
Virtual access subinterface creation is globally...	Configured setting of the **virtual-template** command. Virtual access subinterface creation can be enabled or disabled.
Active Interface	Number of virtual access interfaces that are cloned from the specified virtual template.
Active Subinterface	Number of virtual access subinterfaces that are cloned from the specified virtual template.
Subint Capable	Specifies if the configuration of the virtual template is supported on the virtual access subinterface.
Pre-clone Available	Number of precloned virtual access interfaces currently available for use for the particular virtual template.
Pre-clone Limit	Number of precloned virtual access interfaces available for that particular virtual template.
Current in use	Number of virtual access interfaces and subinterfaces that are currently in use.
Current free	Number of virtual access interfaces and subinterfaces that are no longer in use.
Total	Total number of virtual access interfaces and subinterfaces that exist.
Cumulative created	Number of requests for a virtual access interface or subinterface that have been satisfied.

Field	Description
Cumulative freed	Number of times that the application using the virtual access interface or subinterface has been freed.
Base virtual-access interfaces	Specifies the number of base virtual access interfaces. The base virtual access interface is used to create virtual access subinterfaces. There is one base virtual access interface per application that supports subinterfaces. A base virtual access interface can be identified from the output of the **show interfaces virtual-access** command.
Total create or clone requests	Number of requests that have been made through the asynchronous request API of the virtual template manager.
Current request queue size	Number of items in the virtual template manager work queue.
Current free pending	Number of virtual access interfaces whose final freeing is pending. These virtual access interfaces cannot currently be freed because they are still in use.
Maximum request duration	Maximum time that it took from the time that the asynchronous request was made until the application was notified that the request was done.
Average request duration	Average time that it took from the time that the asynchronous request was made until the application was notified that the request was done.
Last request duration	Time that it took from the time that the asynchronous request was made until the application was notified that the request was done for the most recent request.
Maximum processing duration	Maximum time that the virtual template manager spent satisfying the request.
Average processing duration	Average time that the virtual template manager spent satisfying the request.
Last processing duration	Time that the virtual template manager spent satisfying the request for the most recent request.

Related Commands

Command	Description
clear counters	Clears interface counters.

Command	Description
show interfaces virtual-access	Displays status, traffic data, and configuration information about a specified virtual access interface.
virtual-template	Specifies which virtual template will be used to clone virtual access interfaces.

show vtemplate redundancy

To display 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 **show vtemplate redundancy** command in privileged EXEC mode.

show vtemplate redundancy

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

Use the **clear vtemplate redundancy counters** command on either the Active or Standby route processor (RP), to clear all counters.

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 will increment the “failed” or “error” counters.

The table below describes significant fields shown in this output.

Table 30 show vtemplate redundancy Field Descriptions

Field	Description
Vaccess dynamic sync send	Increments when Active RP synchronizes each virtual template, as it is created, to the Standby RP.
Vaccess dynamic sync send failed	Increments when Vaccess dynamic sync send actions fail.
Vaccess bulk sync send	Increments to the total number of existing virtual templates, when the newly Active RP (post failover or switchover) has synchronized all the existing virtual templates to the new Standby RP.
Vaccess bulk sync send failed	Increments if Vaccess bulk sync send actions fail.
Vaccess sync rcvd on standby	Increments to reflect the total number of dynamic and bulk synchronization send values, the Standby RP reported back to the Active RP.
Vaccess recreate error on standby	Increments if the Standby RP is unable to process synchronization messages from the Active RP.

Related Commands

Command	Description
clear vtemplate redundancy counters	Clears synchronization counters between the Active and Standby RPs.

snmp-server enable traps vpdn dead-cache

To enable the sending of a Simple Network Management Protocol (SNMP) message notification when an L2TP network server (LNS) enters or exits a dead-cache (DOWN) state, use the **snmp-server enable traps vpdn dead-cache** command in global configuration mode. To disable the SNMP notifications, use the **no** form of this command.

snmp-server enable traps vpdn dead-cache

no snmp-server enable traps vpdn dead-cache

Syntax Description

This command has no arguments or keywords.

Command Default

SNMP notification is disabled.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables SNMP trap events.

This command controls (enables or disables) an SNMP message notification when an LNS exits or enters the dead-cache state. SNMP are status notification messages that are generated by the routing device during operation. These messages are typically logged to a destination (such as the terminal screen, to a system buffer, or to a remote host).

You can use the **show vpdn dead-cache** command to view an LNS entry in the dead-cache state.

You can use the **clear vpdn dead-cache** command to clear an LNS entry in the dead-cache state.

Examples

The following example enables the router to send an SNMP message when an LNS enters or exits a dead-cache state:

```
Router(config)# snmp-server enable traps vpdn dead-cache
```

Related Commands

Command	Description
clear vpdn dead-cache	Clears an LNS entry in a dead-cache state.
show vpdn dead-cache	Displays LNS entries in a dead-cache state.

source-ip

To specify an IP address that is different from the physical IP address used to open a virtual private dialup network (VPDN) tunnel for the tunnels associated with a VPDN group, use the **source-ip** command in VPDN group configuration mode. To remove the alternate IP address, use the **no** form of this command.

source-ip *ip-address*

no source-ip

Syntax Description

ip-address	Alternate IP address.

Command Default

No alternate IP address is specified.

Command Modes

VPDN group configuration (config-vpdn)

Command History

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

Usage Guidelines

Use the **source-ip** command in VPDN group configuration mode to configure an alternate IP address to be used for only those tunnels associated with that VPDN group. Each VPDN group on a router can be configured with a unique **source-ip** command.

Use the **vpdn source-ip** command to specify a single alternate IP address to be used for all tunnels on the device. A single source IP address can be configured globally per device.

The VPDN group-level configuration will override the global configuration.

Examples

The following example configures a network access server (NAS) to accept Layer 2 Tunneling Protocol (L2TP) dial-out calls using the alternate IP address 172.23.33.7, which is different from the physical IP address used to open the L2TP tunnel:

```
vpdn-group 3
 accept-dialout
  protocol l2tp
  dialer 2
 terminate-from hostname router21
 source-ip 172.23.33.7
```

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 dial-in 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 dial-out 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 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.
vpdn source-ip	Globally specifies an IP address that is different from the physical IP address used to open a VPDN tunnel.

source vpdn-template

To associate a virtual private dialup network (VPDN) group with a VPDN template, use the **source vpdn-template** command in VPDN group configuration mode. To disassociate a VPDN group from a VPDN template, use the **no** form of this command.

source vpdn-template [*name*]

no source vpdn-template [*name*]

Syntax Description

name	(Optional) The name of the VPDN template to be associated with the VPDN group.

Command Default

Global VPDN template settings are applied to individual VPDN groups if a global VPDN template has been defined. If no global VPDN template has been defined, system default settings are applied to individual VPDN groups.

Command Modes

VPDN group configuration (config-vpdn)

Command History

Release	Modification
12.2(4)B	This command was introduced on the Cisco 7200 series and Cisco 7401ASR routers.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T without support for the *name* argument.
12.2(13)T	Support was added for the *name* argument in 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 **source vpdn-template** command to associate a VPDN group with a VPDN template. By default, VPDN groups are associated with the global VPDN template if one is defined. A VPDN group can be associated with only one VPDN template. Associating a VPDN group with a named VPDN template automatically disassociates it from the global VPDN template.

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

- VPDN parameters configured for the individual VPDN group are always applied to that VPDN group.

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

Disassociating a VPDN group from the global VPDN template by using the **no source vpdn-template** command results in the following hierarchy for the application of VPDN parameters to that VPDN group:

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

If you disassociate a VPDN group from a named VPDN template, the VPDN group is associated with the global VPDN template if one is defined.

Examples

The following example configures the VPDN group named group1 to ignore the global VPDN template settings and use the system default settings for all unspecified VPDN parameters:

```
Router(config)# vpdn-group group1
Router(config-vpdn)# no source vpdn-template
```

The following example creates a VPDN template named l2tp, enters VPDN template configuration mode, configures two VPDN parameters in the VPDN template, and associates the VPDN group named l2tptunnels with the VPDN template:

```
Router(config)# vpdn-template l2tp
Router(config-vpdn-templ)# l2tp tunnel busy timeout 65
Router(config-vpdn-templ)# l2tp tunnel password 7 tunnel4me
!
Router(config)# vpdn-group l2tptunnels
Router(config-vpdn)# source vpdn-template l2tp
```

The following example disassociates the VPDN group named l2tptunnels from the VPDN template named l2tp. The VPDN group is associated with the global VPDN template if one has been defined.

```
Router(config)# vpdn-group l2tptunnels
Router(config-vpdn)# no source vpdn-template l2tp
```

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.

sso enable

To enable the Layer 2 Tunneling Protocol (L2TP) high-availability (HA) operability on virtual private dial-in network (VPDN) groups, use the **sso enable** command in VPDN group configuration mode. To disable L2TP HA operability, use the **no** form of this command.

sso enable

no sso enable

Syntax Description

This command has no arguments or keywords.

Command Default

SSO is enabled.

Command Modes

VPDN group configuration (config-vpdn)

Command History

Release	Modification
Cisco IOS XE Release 2.2	This command was introduced.

Usage Guidelines

This command is enabled by default and is hidden from the output of the **show running-config** command.

Use the **no sso enable** command to disable L2TP High Availability (HA) for any VPDN group. If you disable L2TP HA by using the **no l2tp sso enable** command, L2TP HA functionality is also disabled for all VPDN groups.

Use the **debug l2tp redundancy** and the **debug vpdn redundancy** commands in privileged EXEC mode to display a list L2TP HA checkpointed events and errors.

Use the **show l2tp redundancy** command in privileged EXEC mode to display L2TP checkpointed status information.

Examples

The following example shows how to disable L2TP HA functionality for the VPDN group named *example*:

```
Router# configure terminal
Router(conf)# vpdn enable
Router(conf-vpdn)# vpdn-group example
Router(conf-vpdn)# no sso enable
```

Related Commands

Command	Description
debug l2tp redundancy	Displays information on L2TP sessions having redundancy events and errors.
debug vpdn redundancy	Displays information on VPDN sessions having redundancy events and errors.
l2tp sso enable	Enables L2TP HA.
l2tp tunnel resync	Specifies the number of packets sent before waiting for an acknowledgment message.
show l2tp redundancy	Displays L2TP sessions containing redundancy data.
show vpdn redundancy	Displays VPDN sessions containing redundancy data.

substitute (control policy-map class)

To match the contents, stored in temporary memory of identifier types received by the policy manager, against a specified *matching-pattern* and to perform the substitution defined in a *rewrite-pattern*, use the **substitite** command in configuration-control-policymap-class configuration mode. To disable the substitution of regular expressions, use the **no** form of this command.

action-number **substitute** *variable matching-pattern rewrite-pattern*

no *action-number* **substitute** *variable matching-pattern rewrite-pattern*

Syntax Description

action-number	Number of the action. Actions are executed sequentially within the policy rule.
variable	Uses the contents in the temporary memory storage designated by a variable (created by a set command) for substitution and stores the results of the substitution in the same temporary memory.
matching-pattern	A regular expression. Rejected if the *matching-pattern* value violates any regular expression syntax rules.
rewrite-pattern	A string containing back-referenced characters \0 through \9 that is replaced by strings that match by the whole of, or the 1st to 9th parenthetical part of *matching-pattern.*. The pattern matching method is the longest matching first.

Command Default

The control policy will not initiate substitution.

Command Modes

Configuration-control-policymap-class configuration

Command History

Release	Modification
12.2(31)SB2	This command was introduced.

Usage Guidelines

The **substitute** command allows you to match the contents of a *variable* by using a *matching-pattern* value and perform the substitution defined in a *rewrite-pattern.*. This command is rejected if the *variable* value is not present in a preceding **set** action in the same control-policy class map, or if the *matching-pattern* value violates any regular expression syntax rules.

Examples

The following example shows the policy map with the substitute statement 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
authenticate	Initiates an authentication request for an ISG subscriber session.
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.

tacacs-server domain-stripping

To configure a network access server (NAS) to strip suffixes, or to strip both suffixes and prefixes from the username before forwarding the username to the remote TACACS+ server, use the **tacacs-server domain-stripping** command in global configuration mode. To disable a stripping configuration, use the **no** form of this command.

tacacs-server domain-stripping [[**right-to-left**] [**prefix-delimiter** *character* [*character2 ... character7*]] [**delimiter** *character* [*character2 ... character7*]] | **strip-suffix** *suffix*] [**vrf** *vrf-name*]

no tacacs-server domain-stripping [[**right-to-left**] [**prefix-delimiter** *character* [*character2 ... character7*]] [**delimiter** *character* [*character2 ... character7*]] | **strip-suffix** *suffix*] [**vrf** *vrf-name*]

Syntax Description

right-to-left	(Optional) Specifies that the NAS applies the stripping configuration at the first delimiter found when parsing the full username from right to left. The default is for the NAS to apply the stripping configuration at the first delimiter found when parsing the full username from left to right.
prefix-delimiter *character* [*character2... character7*]	(Optional) Enables prefix stripping and specifies the character or characters that are recognized as a the prefix delimiter. Valid values for the *character* argument are @, /, $, %, \, #, and -. Multiple characters can be entered without intervening spaces. Up to seven characters can be defined as prefix delimiters, which is the maximum number of valid characters. If a \ is entered as the final or only value for the *character* argument, it must be entered as \\. No prefix delimiter is defined by default.
delimiter *character* [*character2... character7*]	(Optional) Specifies the character or characters that are recognized as a suffix delimiter. Valid values for the *character* argument are @, /, $, %, \, #, and -. Multiple characters can be entered without intervening spaces. Up to seven characters can be defined as suffix delimiters, which is the maximum number of valid characters. If a \ is entered as the final or only value for the *character* argument, it must be entered as \\. The default suffix delimiter is the @ character.
strip-suffix *suffix*	(Optional) Specifies a suffix to strip from the username.
vrf *vrf-name*	(Optional) Restricts the domain stripping configuration to a Virtual Private Network (VPN) routing and forwarding (VRF) instance. The *vrf-name* argument specifies the name of a VRF.

Command Default

Stripping is disabled. The full username is sent to the TACACS+ server.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(4)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
XE 2.5	This command was integrated into Cisco IOS Release XE 2.5.

Usage Guidelines

Use the **tacacs-server domain-stripping** command to configure the NAS to strip the domain from a username before forwarding the username to the TACACS+ server. If the full username is user1@cisco.com, enabling the **tacacs-server domain-stripping** command results in the username *user1* being forwarded to the TACACS+ server.

Use the **right-to-left** keyword to specify that the username should be parsed for a delimiter from right to left, rather than from left to right. This allows strings with two instances of a delimiter to strip the username at either delimiter. For example, if the username is user@cisco.com@cisco.net, the suffix could be stripped in two ways. The default direction (left to right) results in the username *user* being forwarded to the TACACS+ server. Configuring the **right-to-left** keyword results in the username *user@cisco.com* being forwarded to the TACACS+ server.

Use the **prefix-delimiter** keyword to enable prefix stripping and to specify the character or characters that are recognized as a prefix delimiter. The first configured character that is parsed is used as the prefix delimiter, and any characters before that delimiter are stripped.

Use the **delimiter** keyword to specify the character or characters that are recognized as a suffix delimiter. The first configured character that is parsed is used as the suffix delimiter, and any characters after that delimiter are stripped.

Use the **strip-suffix** *suffix* keyword to specify a particular suffix to strip from usernames. For example, configuring the **tacacs-server domain-stripping strip-suffix cisco.net** command results in the username user@cisco.net being stripped, while the username user@cisco.com is not stripped. You can configure multiple suffixes for stripping by issuing multiple instances of the **tacacs-server domain-stripping** command. The default suffix delimiter is the @ character.

Note

> Issuing the **tacacs-server domain-stripping strip-suffix** *suffix* command disables the capacity to strip suffixes from all domains. Both the suffix delimiter and the suffix must match for the suffix to be stripped from the full username. The default suffix delimiter of @ is used if you do not specify a different suffix delimiter or set of suffix delimiters by using the **delimiter** keyword.

Note Issuing the **no tacacs-server host** command reconfigures the TACACS server host information. You can view the contents of the current running configuration file by using the **show running-config** command.

To apply a domain-stripping configuration only to a specified VRF, use the **vrf** *vrf-name* option.

The interactions between the different types of domain stripping configurations are as follows:

- You can configure only one instance of the **tacacs-server domain-stripping** [**right-to-left**] [**prefix-delimiter** *character* [*character2...character7*]] [**delimiter** *character* [*character2...character7*]] command.
- You can configure multiple instances of the **tacacs-server domain-stripping** [**right-to-left**] [**prefix-delimiter** *character* [*character2...character7*]] [**delimiter** *character* [*character2...character7*]] [**vrf** *vrf-name*] command with unique values for **vrf** *vrf-name*.
- You can configure multiple instances of the **tacacs-server domain-stripping strip-suffix** *suffix* [**vrf** *vrf-name*] command to specify multiple suffixes to be stripped as part of a global or per-VRF ruleset.
- Issuing any version of the **tacacs-server domain-stripping** command automatically enables suffix stripping by using the default delimiter character @ for that ruleset, unless a different delimiter or set of delimiters is specified.
- Configuring a per-suffix stripping rule disables generic suffix stripping for that ruleset. Only suffixes that match the configured suffix or suffixes are stripped from usernames.

Examples

The following example shows how to configure the router to parse the username from right to left and set the valid suffix delimiter characters as @, \, and $. If the full username is cisco/user@cisco.com$cisco.net, the username “cisco/user@cisco.com” is forwarded to the TACACS+ server because the $ character is the first valid delimiter encountered by the NAS when parsing the username from right to left.

```
tacacs-server domain-stripping right-to-left delimiter @\$
```

The following example shows how to configure the router to strip the domain name from usernames only for users associated with the VRF instance named abc. The default suffix delimiter @ is used for generic suffix stripping.

```
tacacs-server domain-stripping vrf abc
```

The following example shows how to enable prefix stripping using the character / as the prefix delimiter. The default suffix delimiter character @ is used for generic suffix stripping. If the full username is cisco/user@cisco.com, the username "user" is forwarded to the TACACS+ server.

```
tacacs-server domain-stripping prefix-delimiter /
```

The following example shows how to enable prefix stripping, specify the character / as the prefix delimiter, and specify the character # as the suffix delimiter. If the full username is cisco/user@cisco.com#cisco.net, the username "user@cisco.com" is forwarded to the TACACS+ server.

```
tacacs-server domain-stripping prefix-delimiter / delimiter #
```

The following example shows how to enable prefix stripping, configure the character / as the prefix delimiter, configure the characters $, @, and # as suffix delimiters, and configure per-suffix stripping of the suffix cisco.com. If the full username is cisco/user@cisco.com, the username "user" is forwarded to the

TACACS+ server. If the full username is cisco/user@cisco.com#cisco.com, the username "user@cisco.com" is forwarded.

```
tacacs-server domain-stripping prefix-delimiter / delimiter $@#
tacacs-server domain-stripping strip-suffix cisco.com
```

The following example shows how to configure the router to parse the username from right to left and enable suffix stripping for usernames with the suffix cisco.com. If the full username is cisco/user@cisco.net@cisco.com, the username "cisco/user@cisco.net" is forwarded to the TACACS+ server. If the full username is cisco/user@cisco.com@cisco.net, the full username is forwarded.

```
tacacs-server domain-stripping right-to-left
tacacs-server domain-stripping strip-suffix cisco.com
```

The following example shows how to configure a set of global stripping rules that strip the suffix cisco.com by using the delimiter @, and a different set of stripping rules for usernames associated with the VRF named myvrf:

```
tacacs-server domain-stripping strip-suffix cisco.com
!
tacacs-server domain-stripping prefix-delimiter # vrf myvrf
tacacs-server domain-stripping strip-suffix cisco.net vrf myvrf
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.
ip vrf	Defines a VRF instance and enters VRF configuration mode.
radius-server domain-stripping	Configures a router to strip a prefix or suffix from the username before forwarding the username to the RADIUS server.

terminate-from

To specify the hostname of the remote L2TP access concentrator (LAC) or L2TP network server (LNS) that will be required when accepting a virtual private dialup network (VPDN) tunnel, use the **terminate-from** command in VPDN group configuration mode. To remove the hostname from the VPDN group, use the **no**form of this command.

terminate-from hostname *host-name*

no terminate-from [**hostname** *host-name*]

Syntax Description

hostname *host-name*	Hostname from which this VPDN group will accept connections.

Command Default

Disabled

Command Modes

VPDN group configuration

Command History

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

Usage Guidelines

Before you can use this command, you must have already enabled one of the two accept VPDN subgroups by using either the **accept-dialin**or **accept-dialout** command.

Each VPDN group can only terminate from a single hostname. If you enter a second **terminate-from** command on a VPDN group, it will replace the first **terminate-from** command.

Examples

The following example configures a VPDN group to accept L2TP tunnels for dial-out calls from the LNS cerise by using dialer 2 as its dialing resource:

```
vpdn-group 1
 accept-dialout
 protocol l2tp
 dialer 2
terminate-from hostname host1
```

Related Commands

Command	Description
accept-dialin	Specifies the LNS to use for authenticating, and the virtual template to use for cloning, new virtual access interfaces when an incoming L2TP tunnel connection is requested from a specific peer.
accept-dialout	Accepts requests to tunnel L2TP dial-out calls and creates an accept-dialout VPDN subgroup

U through Z

virtual-template

To specify which virtual template is used to clone virtual access interfaces (VAI), use the **virtual-template** command in BBA group configuration mode and in VPDN group configuration mode. To remove the virtual template from a virtual private dialup network (VPDN) group, use the **no** form of this command.

virtual-template *template-number*

no virtual-template

Syntax Description

template-number	Number of the virtual template that will be used to clone VAIs. The range is 1 to 1000.

Command Default

No virtual template is enabled.

Command Modes

BBA group configuration mode (config-bba-group)

VPDN group configuration (config-vpdn)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.1(1)T	This command was enhanced to enable PPPoE on ATM to accept dial-in PPP over Ethernet (PPPoE) sessions.
12.2(15)T	This command was enhanced to allow IP per-user attributes to be applied to a Layer 2 Tunneling Protocol (L2TP) dial-out session.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command’s default configuration was modified and implemented on the Cisco 10000 series router for the PRE3 and PRE4 as described in the "Usage Guidelines" section.
Cisco IOS XE Release 2.5	This command was implemented on Cisco ASR 1000 series routers.

Usage Guidelines

You must first enable a tunneling protocol on the VPDN group by using the **protocol** (VPDN) command before you can enable the **virtual-template** command. Removing or modifying the **protocol** command removes the **virtual-template** command from the VPDN group.

Each VPDN group can clone only VAIs using one virtual template. If you enter a second **virtual-template** command on a VPDN group, it replaces the first **virtual-template** command.

The table below lists the VPDN group commands under which the **virtual-template** command can be entered. Entering the VPDN group command starts VPDN group configuration mode. The table includes the command-line prompt for the VPDN group configuration mode and the type of service configured.

Table 31 VPDN Subgroups

VPDN Group Command	Command Mode Prompt	Type of Service
accept-dialin	`router(config-vpdn-acc-in)#`	Tunnel server
request-dialout	`router(config-vpdn-req-out)#`	L2TP network server (LNS)

When the **virtual-template** command is entered under a **request-dialout** VPDN subgroup, IP and other per-user attributes can be applied to an L2TP dial-out session from an LNS. Before this command was enhanced, IP per-user configurations from authentication, authorization, and accounting (AAA) servers were not supported; the IP configuration comes from the dialer interface defined on the router.

The enhanced **virtual-template** command works in a way similar to configuring virtual profiles and L2TP dial-in. The L2TP VAI is first cloned from the virtual template, which means that configurations from the virtual template interface is applied to the L2TP VAI. After authentication, the AAA per-user configuration is applied to the VAI. Because AAA per-user attributes are applied only after the user has been authenticated, the LNS must be configured to authenticate the dial-out user (configuration authentication is needed for this command).

With the enhanced **virtual-template** command, all software components can now use the configuration present on the VAI rather than what is present on the dialer interface. For example, IP Control Protocol (IPCP) address negotiation uses the local address of the VAI as the router address while negotiating with the peer.

Cisco 10000 Series Router Usage Guidelines

In Cisco IOS Release 12.2(33)SB, the **virtual-template snmp** command has a new default configuration. Instead of being enabled by default, **no virtual-template snmp** is the default configuration. This setting enhances scaling and prevents large numbers of entries in 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 enables the LNS to accept an L2TP tunnel from an L2TP access concentrator (LAC) named LAC2. A VAI will be cloned from virtual template 1.

```
vpdn-group 1
 accept-dialin
  protocol l2tp
  virtual-template 1
 terminate-from hostname LAC2
```

The following example enables PPPoE on ATM to accept dial-in PPPoE sessions. A VAI for the PPP session is cloned from virtual template 1.

```
vpdn-group 1
 accept-dialin
  protocol pppoe
  virtual-template 1
```

The following partial example shows how to configure an LNS to support IP per-user configurations from a AAA server:

```
!
vpdn enable
vpdn search-order domain
!
vpdn-group 1
.
.
.
 request-dialout
  protocol l2tp
  rotary-group 1
  virtual-template 1
 initiate-to ip 10.0.1.194.2
 local name lns
 l2tp tunnel password 7094F3$!5^3
 source-ip 10.0.194.53
!
```

The previous configuration requires a AAA profile such as the following example to specify the per-user attributes:

```
5300-Router1-out  Password = "cisco"
     Service-Type = Outbound
     cisco-avpair = "outbound:dial-number=5550121"
7200-Router1-1  Password = "cisco"
     Service-Type = Outbound
     cisco-avpair = "ip:route=10.17.17.1 255.255.255.255 Dialer1 100 name 5300-Router1"
5300-Router1 Password = "cisco"
     Service-Type = Framed
     Framed-Protocol = PPP
     cisco-avpair = "lcp:interface-config=ip unnumbered loopback 0"
     cisco-avpair = "ip:outacl#1=deny ip host 10.5.5.5 any log"
     cisco-avpair = "ip:outacl#2=permit ip any any"
     cisco-avpair = "ip:inacl#1=deny ip host 10.5.5.5 any log"
     cisco-avpair = "ip:inacl#2=permit ip any any"
     cisco-avpair = "multilink:min-links=2"
     Framed-Route = "10.5.5.6/32 Ethernet4/0"
     Framed-Route = "10.5.5.5/32 Ethernet4/0"
     Idle-Timeout = 100
```

Related Commands

Command	Description
accept-dialin	Configures an LNS to accept tunneled PPP connections from a LAC and to create an accept-dialin VPDN subgroup.
protocol (VPDN)	Specifies the Layer 2 Tunneling Protocol that the VPDN subgroup will use.
request-dialout	Enables an LNS to request VPDN dial-out calls by using L2TP and to create a request-dialout VPDN subgroup.
show vtemplate	Displays information about all configured virtual templates.
vpdn-group	Defines a local, unique group number identifier.

vpdn aaa attribute

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

vpdn aaa attribute {**nas-ip-address** {**vpdn-nas** | **vpdn-tunnel-client**} | **nas-port** {**physical-channel-id** | **vpdn-nas**}}

no vpdn aaa attribute {**nas-ip-address** {**vpdn-nas** | **vpdn-tunnel-client**} | **nas-port**}

Syntax Description

nas-ip-address vpdn-nas	Enables reporting of the VPDN NAS IP address to the AAA server.
nas-ip-address vpdn-tunnel-client	Enables reporting of the VPDN tunnel client IP address to the AAA server.
nas-port vpdn-nas	Enables reporting of the VPDN NAS port to the AAA server.
nas-port physical-channel-id	Enables reporting of the VPDN NAS port physical channel identifier to the AAA server.

Command Default

AAA attributes are not reported to the AAA server.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.3NA	This command was introduced.
11.3(8.1)T	This command was integrated into Cisco IOS Release 11.3(8.1)T.
12.1(5)T	This command was modified to support the PPP extended NAS-Port format.
12.2(13)T	The **physical-channel-id** keyword was added
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
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.
12.4(24)T	The **vpdn-tunnel-client** keyword was added.
12.2(33)XND	The **vpdn-tunnel-client** keyword was added.
12.2(33)SRE	The **vpdn-tunnel-client** keyword was added.
Cisco IOS XE Release 2.5	The **vpdn-tunnel-client** keyword was added.

Usage Guidelines

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

The PPP extended NAS-Port format enables the NAS-Port and NAS-Port-Type attributes to provide port details to a RADIUS server when one of the following protocols is configured:

- PPP over ATM
- PPP over Ethernet (PPPoE) over ATM
- PPPoE over 802.1Q VLANs

Before PPP extended NAS-Port format attributes can be reported to the RADIUS server, the **radius-server attribute nas-port format** command with the **d** keyword must be configured on both the tunnel server and the NAS, and the tunnel server and the NAS must both be Cisco routers.

When you configure the **vpdn aaa attribute nas-ip-address vpdn-nas** command, the L2TP network server (LNS) reports the IP address of the last multihop node for multihop over Layer 2 Forwarding (L2F). For multihop over Layer 2 Tunneling Protocol (L2TP), the IP address of the originating NAS is reported.

When you configure the **vpdn aaa attribute nas-ip-address vpdn-tunnel-client** command, the LNS reports the IP address of the last multihop node in the RADIUS NAS-IP-Address attribute for the L2TP multihop. This eases the migration for customers moving from L2F to L2TP.

Note

Reporting of NAS AAA attributes related to a VPDN on a AAA server is not supported for Point-to-Point Tunneling Protocol (PPTP) sessions with multihop deployment.

Examples

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

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

The following example configures the tunnel server for VPDN, enables AAA, configures a RADIUS AAA server, and enables reporting of PPP extended NAS-Port format values to the RADIUS server. PPP extended NAS-Port format must also be configured on the NAS for this configuration to be effective.

```
vpdn enable
vpdn-group L2TP-tunnel
 accept-dialin
  protocol l2tp
  virtual-template 1
!
 terminate-from hostname nas1
 local name ts1
!
aaa new-model
aaa authentication ppp default local group radius
aaa authorization network default local group radius
aaa accounting network default start-stop group radius
!
radius-server host 172.16.79.76 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server attribute nas-port format d
radius-server key ts123
!
vpdn aaa attribute nas-port vpdn-nas
```

Related Commands

Command	Description
radius-server attribute nas-port format	Selects the NAS-Port format used for RADIUS accounting features.

vpdn aaa override-server

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

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

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

Syntax Description

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

Command Default

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

Command Modes

Global configuration (config)

Command History

Release	Modification
11.2 F	This command was introduced.

Usage Guidelines

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

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

Examples

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

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

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.
tacacs-server directed-request	Sends only a username to a specified server when a direct request is issued.
vpdn enable	Enables VPDN on the router and directs the router to look for tunnel definitions in a local database and on a remote authorization server (home gateway), if one is present.

vpdn aaa untagged

To apply untagged attribute values obtained from the authentication, authorization, and accounting (AAA) RADIUS server to all attribute sets for virtual private dialup network (VPDN) tunnels, use the **vpdn aaa untagged** command in global configuration mode. To disable this function, use the **no** form of this command.

vpdn aaa untagged default

no vpdn aaa untagged default

Syntax Description

default	Sets the untagged attribute value as default.

Command Default

Untagged attribute values are applied to all attribute sets.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(1)T	This command was introduced.
15.0(1)M	This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The **default** keyword was added.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

Untagged attribute values obtained from the AAA RADIUS server are applied to all attribute sets by default, unless a value for that attribute is already specified in the tagged attribute set. To prevent untagged attribute values from being applied to tagged attribute sets, use the **no** form of this command.

Examples

The following example shows how to disable the application of untagged attribute values to attribute sets:

```
Router# configure terminal
Router(config)# no vpdn aaa untagged default
```

Related Commands

Command	Description
show vpdn	Displays basic information about all active VPDN tunnels.

vpdn authen-before-forward

Note Effective with Cisco Release 12.4(11)T, the support for L2F was removed in Cisco IOS Software.

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

vpdn authen-before-forward

no vpdn 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

Global configuration (config)

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

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.

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.

Enabling the **vpdn 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 32 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 the NAS to request authentication of all dial-in L2TP or L2F sessions before the sessions are forwarded to the tunnel server:

```
vpdn authen-before-forward
```

Related Commands

Command	Description
authen-before-forward	Configures a NAS to request authentication of a complete username before making a forwarding decision for dial-in L2TP or L2F tunnels belonging to a VPDN group.

vpdn authorize directed-request

To enable virtual private dialup network (VPDN) authorization for directed-request users, use the **vpdn authorize directed-request** command in global configuration mode. To disable VPDN authorization for directed request users, use the **no** form of this command.

vpdn authorize directed-request

no vpdn authorize directed-request

Syntax Description

This command has no keywords or arguments.

Command Default

VPDN authorization for directed-request users is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1	This command was introduced.

Usage Guidelines

When a username includes both a username and a domain portion, such as user@site.com, directed request configuration allows the authorization request to be sent to a specific RADIUS or TACACS+ server based on the domain name portion of the username (site.com). The **vpdn authorize directed-request** command must be enabled to allow VPDN authorization of any directed request user.

Directed request for RADIUS users is enabled by issuing the **radius-server directed-request** command. Directed request for TACACS+ users is enabled by default, and can be disabled by using the **no tacacs-server directed request** command. The **ip host** command must be configured to enable directed requests to RADIUS or TACACS+ servers.

The **vpdn authorize directed-request** command is usually configured on the L2TP network server (LNS). When directed-requests are used on an L2TP access concentrator (LAC) with per-user VPDN configuration, the **authen before-forward** command must be enabled.

Examples

The following example enables VPDN authorization and RADIUS directed requests on an LNS:

```
ip host site.com 10.1.1.1
radius-server host 10.1.1.1 auth-port 1645 acct-port 1646
radius-server directed-request
vpdn authorize directed-request
```

The following example enables VPDN authorization and TACACS+ directed requests on an LNS:

```
ip host site.com 10.1.1.1
tacacs-server host 10.1.1.1
tacacs-server directed-request
vpdn authorize directed-request
```

The following example enables per-user VPDN and enables VPDN authorization for directed request users on a LAC:

```
vpdn-group 1
 request-dialin
  protocol l2f
  domain cisco.com
 !
 initiate-to ip 10.1.1.1
 local name local1
 authen before-forward
!
ip host cisco.com 10.1.1.1
vpdn authorize directed-request
!
radius-server host 10.1.1.1 auth-port 1645 acct-port 1646
radius-server directed-request
```

Related Commands

Command	Description
authen before-forward	Specifies that the VPDN sends the entire structured username to the AAA server the first time the router contacts the AAA server.
ip host	Defines a static hostname-to-address mapping in the host cache.
radius-server directed-request	Allows users logging into a Cisco NAS to select a RADIUS server for authentication.
tacacs-server directed-request	Sends only a username to a specified server when a direct request is issued.

vpdn authorize domain

To enable domain preauthorization on a network access server (NAS), use the **vpdn authorize domain** command in global configuration mode. To disable domain preauthorization, use the **no** form of this command.

vpdn authorize domain

no vpdn authorize domain

Syntax Description

This command has no arguments or keywords.

Command Default

Domain preauthorization is disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(1)DC1	This command was introduced on the Cisco 6400 NRP.
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

A domain preauthorization RADIUS user profile must also be created. See the Examples section and refer to the *Cisco IOS Security Configuration Guide* for information on how to create these profiles.

Examples

Domain Preauthorization Configuration on the LAC Example

The following example shows the configuration necessary for an L2TP access concentrator (LAC) to participate in domain preauthorization:

```
!
aaa new-model
aaa authorization network default local group radius
!
vpdn authorize domain
!
```

```
radius-server host 10.9.9.9 auth-port 1645 acct-port 1646
radius-server attribute nas-port format d
radius-server key MyKey
radius-server vsa send authentication
!
```

Domain Preauthorization RADIUS User Profile Example

The following example shows a domain preauthorization RADIUS user profile:

```
user = nas-port:10.9.9.9:0/0/0/30.33{
 profile_id = 826
 profile_cycle = 1
 radius=Cisco {
 check_items= {
 2=cisco
 }
 reply_attributes= {
 9,1="vpdn:vpn-domain-list=net1.com,net2.com"
 6=5
 }
 }
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.

vpdn domain-delimiter

To specify the characters to be used to delimit the domain prefix or domain suffix, use the **vpdn domain-delimiter** command in global configuration mode. To disable this function, use the **no** form of this command.

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

no vpdn domain-delimiter *characters* [**suffix** | **prefix**]

Syntax Description

characters	One or more specific characters to be used as suffix or prefix delimiters. Available characters are **%**, **-**, **@**, \ , **#**, and **/**. If a backslash (\\) is the last delimiter in the command line, enter it as a double backslash (\\\\).
suffix | **prefix**	(Optional) Usage of the specified characters.

Command Default

Disabled

Command Modes

Global configuration (config)

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

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

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

cisco-avpair = "lcp:interface-config=ip address 10.1.1.1 255.255.255.255.0",

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

Examples

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

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

This example allows the following host and domain names:

```
cisco.com#localddr
localddr@cisco.com
```

Related Commands

Command	Description
vpdn enable	Enables VPDN on the router and directs the router to look for tunnel definitions in a local database and on a remote authorization server (home gateway), if one is present.
vpdn history failure	Enables logging of VPDN failures to the history failure table or to sets the failure history table size.
vpdn profile	Specifies how the network access server for the service provider is to perform VPDN tunnel authorization searches.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.

vpdn enable

To enable virtual private dialup networking (VPDN) on the router and inform the router to look for tunnel definitions in a local database and on a remote authorization server (home gateway), if one is present, use the **vpdn enable** command in global configuration mode. To disable, use the **no** form of this command.

vpdn enable

no vpdn enable

Syntax Description

This command has no arguments or keywords.

Command Default

VPDN is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SB	This command's behavior was modified and implemented on the Cisco 10000 series router as described in the Usage Guidelines below.

Usage Guidelines

The **no vpdn enable** command does not automatically disable a VPDN tunnel.

To shut down a VPDN tunnel, use the **clear vpdn tunnel** command or the **vpdn softshut** command.

Cisco 10000 Series Usage Guidelines

In Cisco IOS Release 12.2(33)SB and later releases, the router no longer accepts the **vpdn-group** command if you issue the command before you issue the **vpdn enable** command. Instead, the following warning message displays:

```
% VPDN configuration is not allowed until VPDN is enabled through 'vpdn enable'.
```

In releases prior to Cisco IOS Release 12.2(33)SB, if you issue the **vpdn-group** command before the **vpdn enable** command, the router accepts the command and displays the following warning message:

```
% VPDN is not enabled
```

Examples

The following example enables VPDN on the router:

```
vpdn enable
```

Related Commands

Command	Description
clear vpdn tunnel	Shuts down a specified tunnel and all sessions within the tunnel.
vpdn history failure	Enables logging of VPDN failures to the history failure table or to sets the failure history table size.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.
vpdn softshut	Prevents new sessions from being established on a VPDN tunnel without disturbing existing sessions.

vpdn group

To associate a virtual private dialup network (VPDN) group with a customer or VPDN profile, use the **vpdn group** command in customer profile or in VPDN profile configuration mode. To disassociate a VPDN group from a customer or VPDN profile, use the **no** form of this command.

vpdn group *name*

no vpdn group *name*

Syntax Description

name	Name of the VPDN group. **Note** This name should match the name defined for the VPDN group configured with the **vpdn-group** command.

Command Default

No default behavior or values.

Command Modes

Customer profile configuration

VPDN profile configuration (config-vpdn-profile)

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

Use the **vpdn group** command in customer profile configuration mode or in VPDN profile configuration mode to associate a VPDN group with a customer profile or a VPDN profile, respectively.

VPDN groups are created by using the **vpdn-group** command in global configuration mode.

Examples

The following example creates the VPDN groups named l2tp and l2f and associates both VPDN groups with the VPDN profile named profile32:

```
Router(config)# vpdn-group l2tp
Router(config-vpdn)#
!
Router(config)# vpdn-group l2f
Router(config-vpdn)#
!
Router(config)# resource-pool profile vpdn profile32
Router(config-vpdn-profile)# vpdn group l2tp
Router(config-vpdn-profile)# vpdn group l2f
```

The following example creates two VPDN groups and configures them under a customer profile named company2:

```
Router(config)# vpdn-group mygroup
Router(config-vpdn)#
!
Router(config)# vpdn-group yourgroup
Router(config-vpdn)#
!
Router(config)# resource-pool profile vpdn company2
Router(config-vpdn-profile)# vpdn group mygroup
Router(config-vpdn-profile)# vpdn group yourgroup
```

Related Commands

Command	Description
resource-pool profile customer	Creates a customer profile and enters customer profile configuration mode.
resource-pool profile vpdn	Creates a VPDN profile and enters VPDN profile configuration mode.
vpdn profile	Associates a VPDN profile with a customer profile.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.

vpdn history failure

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

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

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

Syntax Description

table-size *entries*	(Optional) Sets the number of entries in the history failure table. The range is 20 to 50.

Command Default

VPDN failures are logged by default. The table size is 20 entries

Command Modes

Global configuration (config)

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

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

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

All failure entries for the user are kept chronologically in the history table. Each entry records the relevant information of a failure event. Only the most recent failure event per user, unique to its name and tunnel client ID (CLID), is kept.

When the total number of entries in the table reaches the configured table size, the oldest record is deleted and a new entry is added.

Examples

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

```
no vpdn history failure
```

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

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

Related Commands

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

vpdn history failure cause normal

To prevent the message "The remote server closed the session" from overwriting useful messages in the virtual private dialup network (VPDN) connection failure log, use the **no vpdn history failure cause normal** command in global configuration mode. To reenable logging of the message (the default), use the **vpdn history failure cause normal** command.

vpdn history failure cause normal

no vpdn history failure cause normal

Syntax Description

This command has no arguments or keywords.

Command Default

This command is enabled when the VPDN failure log is enabled, but it does not appear in the configuration of a Layer 2 access concentrator (LAC) or Layer 2 network server (LNS) when the running configuration is listed. When the **no** form of this command is configured, the command be listed in the running configuration. See the "Usage Guidelines" section for more information.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(5a)B1	This command was introduced.
12.3(11)T	This command was integrated into Cisco IOS Release 12.3(11)T.
12.3(4)T8	This command was integrated into Cisco IOS Release 12.3(4)T8.
12.3(7)T3	This command was integrated into Cisco IOS Release 12.3(7)T3.
12.3(8)T6	This command was integrated into Cisco IOS Release 12.3(7)T6.
12.3(7)XI3	This command was integrated into Cisco IOS Release 12.3(7)XI3.

Usage Guidelines

When users are declared as unauthenticated, their termination is recorded in the VPDN failure log. One method for determining why a subscriber cannot establish a PPP session is for the network operator to check the VPDN failure log for connection failure messages. The router can determine and log specific reasons for session termination, such as authentication failure, exceeding the session limit, timer expiration, and so on. However, a peer LAC or LNS sends the message "VPDN-6-CLOSED" to the router for any type of session termination. All other messages at the console and in the failure log appear under abnormal termination at that router, and the message "The remote server closed the session" is also logged in the VPDN connection failure log. So the failure log, which has maximum of 50 messages, gets filled with messages. Once the maximum message length is reached, new messages begin replacing old messages and information about the unauthenticated users is lost.

The **no vpdn logging cause normal** command disables all system logging (syslog) messages with the prefix "VPDN-6-CLOSED." The **no vpdn history failure cause normal** command is used to prevent the message "The remote server closed the session" from being added to the connection failure log.

Both commands are independent so that configuring the **no vpdn logging cause normal** command does not prevent the message "The remote server closed the session" from being logged. And conversely, configuring the **no vpdn history failure cause normal** command does not prevent the syslog message "VPDN-6-CLOSED" from appearing.

By default, the **vpdn logging cause normal** command is enabled only when VPDN logging is enabled and does not appear in the **show running-config** command display. When configured, the command **no vpdn logging cause normal** appears in the **show running-config** command display only when VPDN logging is enabled.

By default, the **vpdn history failure cause normal** command is enabled only when the VPDN failure log is enabled, and it does not appear in the **show running-config** command display. When configured, the command **no vpdn history failure cause normal** shows up only when the VPDN history log is enabled.

Regardless of whether the **no vpdn logging cause normal** and the **no vpdn history failure cause normal** commands are configured, all other syslog messages except those with prefix "VPDN-6-CLOSED" appear on the console, and the failure table logs all messages except "The remote server closed the session."

Examples

The default behavior of this command enables logging of the message "The remote server closed the session." The following example shows how to disable both the "The remote server closed the session" and "VPDN-6-CLOSED" messages so that the VPDN connection failure log maintains useful messages about session termination:

```
no vpdn logging cause normal
no vpdn history failure cause normal
```

Related Commands

Command	Description
vpdn logging cause normal	Prevents the message "VPDN-6-CLOSED" from overwriting useful messages in the VPDN connection failure log.

vpdn incoming

The **vpdn incoming** command is replaced by the **accept-dialin** command. See the description of the **accept-dialin** command for more information.

vpdn ip udp ignore checksum

Note Effective with Cisco Release 12.4(33)T, the support for L2F is not available in Cisco IOS Software.

To allow the router to ignore User Datagram Protocol (UDP) checksums for Layer 2 Forwarding (L2F) and Layer 2 Tunneling Protocol (L2TP) virtual private dialup network (VPDN) traffic, use the **vpdn ip udp ignore checksum** command in global configuration mode. To disable the ignoring of UDP checksums, use the **no** form of this command.

vpdn ip udp ignore checksum

no vpdn ip udp ignore checksum

Syntax Description

This command has no arguments or keywords.

Command Default

Releases prior to Cisco IOS Release 12.3(13) and 12.3(14)T: UDP checksums are not ignored by default.

Cisco IOS Release 12.3(13) and 12.3(14)T and later releases: UDP checksums are ignored by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.3(13)	This command was modified to be enabled by default.
12.3(14)T	This command was modified to be enabled by default.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

Ignoring UDP checksums is beneficial when the remote tunnel endpoint uses UDP checksums and when you want to use fast switching or Cisco Express Forwarding (CEF). If the remote tunnel endpoint uses UDP checksums and the **vpdn ip udp ignore checksum** command is disabled, all tunnel traffic is process-switched.

In Cisco IOS Release 12.3(13) and Cisco IOS Release 12.3(14)T, this command was modified to be enabled by default.

Cisco 10000 Series Router

When you configure this command, the router directly queues L2TP hello packets and hello acknowledgments to the L2TP control process. We recommend that you configure this command in all scaled LAC and LNS L2TP tunnel configurations.

If you do not configure the **vpdn ip udp ignore checksum** command, the L2TP software sends the packet to UDP to validate the checksum. When too many packets are queued to the IP input process, the router starts selective packet discard (SPD), which causes IP packets to be dropped.

Note Head-of-the-line blocking of the IP input process might occur in other non-L2TP configurations. A flush occurring on an input interface indicates that SPD is discarding packets.

Examples

The following example configures the router to ignore UDP checksums, allowing fast switching or CEF:

```
vpdn ip udp ignore checksum
```

The following example disables the ignoring of UDP checksums on the router:

```
no vpdn ip udp ignore checksum
```

vpdn l2tp attribute

To send the attribute value pairs (AVP) in the session creation packets from the L2TP (Layer 2 Tunneling Protocol) Access Controller (LAC) to the L2TP Network Server (LNS), use the **vpdn l2tp attribute** command in global configuration mode. To disable the sending of AVPs, use the **no** form of this command.

vpdn l2tp attribute {**initial-received-lcp-confreq** | **physical-channel-id**}

no vpdn l2tp attribute {**initial-received-lcp-confreq** | **physical-channel-id**}

Syntax Description

initial-received-lcp-confreq	Specifies that the L2TP incoming call connected (ICCN) packets carry a copy of the Initial Received Link Control Protocol (LCP) configure request (CONFREQ) packet received from the PPP client. The attribute value 26 is added to the ICCN packets that are sent to the LNS.
physical-channel-id	Specifies that the L2TP incoming call request (ICRQ) packets carry the physical channel ID AVP. The attribute value 25 is added to the ICRQ packets that are sent to the LNS.

Command Default

The ICCN and the ICRQ packets do not carry the AVPs to the LNS.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced.

Usage Guidelines

ICRQ and ICCN are the respective first and last of the three message exchanges that are used for establishing sessions with an L2TP tunnel.

Use the **vpdn l2tp attribute initial-received-lcp-confreq** command in global configuration mode to add the Initial Received LCP CONFREQ AVP to the ICCN packets on the LAC.

Use the **vpdn l2tp attribute physical-channel-id** command in global configuration mode to add the Physical Channel ID AVP to the ICRQ packets on LAC.

Examples

The following example shows how to send the Initial Received LCP CONFREQ attribute to the LNS in the ICCN packets:

```
Router(config)# vpdn enable
Router(config)# vpdn l2tp attribute initial-received-lcp-confreq
```

vpdn l2tp attribute clid mask-method

To configure a network access server (NAS) to suppress Layer 2 Tunneling Protocol (L2TP) calling station IDs globally, use the **vpdn l2tp attribute clid mask-method** command in global configuration mode. To disable this function, use the **no** form of this command.

vpdn l2tp attribute clid mask-method {**right** *mask-character characters* | **remove**} [**match** *match-string*]

no vpdn l2tp attribute clid mask-method {**right** *mask-character characters* | **remove**} [**match** *match-string*]

Syntax Description

right	Specifies that the calling station ID will be masked by replacing characters, starting from the right end of the string.
mask-character	Character to be used as a replacement. Only printable characters are accepted.
characters	Number of characters to be replaced.
remove	Specifies that the entire calling station ID will be removed.
match *match-string*	(Optional) Applies the defined masking method only if the string specified by the *match-string* argument is contained in the username.

Command Default

The calling station ID is not masked or dropped.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.3(14)YM2	This command was integrated into Cisco IOS Release 12.3(14)YM2 and implemented on the Cisco 7301, Cisco 7204VXR, and Cisco 7206VXR routers.

Usage Guidelines

Use the **vpdn l2tp attribute clid mask-method** command to mask the calling station ID in L2TP attribute-value (AV) pair 22 globally for all virtual private dialup network (VPDN) groups configured on the NAS. This command is compatible with both local and remote RADIUS authorization. You can either substitute characters for a portion of the calling station ID or remove the entire calling station ID.

The **l2tp attribute clid mask-method** command can be used to mask the calling station ID for calls associated with a specific VPDN group or VPDN template. This command is compatible with only local authorization.

Examples

The following example shows how to use the **vpdn l2tp attribute clid mask-method** command globally to mask the L2TP calling station ID during authorization if the username contains the string #184.

```
vpdn enable
vpdn l2tp attribute clid mask-method right # 255 match #184
vpdn search-order domain
```

Related Commands

Command	Description
l2tp attribute clid mask-method	Configures a NAS to suppress L2TP calling station IDs for sessions associated with a VPDN group or VPDN template.

vpdn logging

To enable the logging of virtual private dialup network (VPDN) events , use the **vpdn logging** command in global configuration mode. To disable the logging of VPDN events, use the **no** form of this command.

vpdn logging [**accounting** | **local** | **remote** | **tunnel-drop** | **user**]

no vpdn logging [**accounting** | **local** | **remote** | **tunnel-drop** | **user**]

Syntax Description

accounting	(Optional) Enables the transmission of VPDN event log messages within an authentication, authorization, and accounting (AAA) accounting record.
local	(Optional) Enables logging of VPDN events to the system message log (syslog) locally.
remote	(Optional) Enables logging of VPDN events to the syslog of the remote tunnel endpoint.
tunnel-drop	(Optional) Enables logging of VPDN tunnel-drop events to the syslog.
user	(Optional) Enables logging of VPDN user events to the syslog.

Command Default

All VPDN event logging is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.3T	This command was introduced.
12.1	The **user** keyword was introduced in Cisco IOS Release 12.1.
12.2(11)T	The **tunnel-drop** keyword was introduced in Cisco IOS Release 12.2(11)T.
12.2(15)T	The **accounting** keyword was introduced in Cisco IOS Release 12.2(15)T.

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

Usage Guidelines

This command controls the logging of VPDN events. By default, all VPDN event logging is disabled.

In Cisco IOS Releases 15.0, 12.2(33)XNE, 12.2(33)SRE, XE 2.5 and later, when you use any keyword with the **vpdn logging** command, the status of the master flag, which is recognized by the configuration element vpdn logging, is evaluated. If all types of vpdn logging are in their default states (the default for the **vpdn logging cause** command is enabled; the defaults for the other VPDN logging types are disabled), the master flag is turned off, causing the VPDN logging CLI to no longer be generated in the **show running-config** display by the nvgen process. If you configure any VPDN logging type to a nondefault state, the master flag is turned on and the **vpdn logging** output is displayed in the **show running-config** command output.

To enable the logging of VPDN events to the syslog of the local or the remote tunnel endpoint router, issue the **vpdn logging** command with the **local** or the **remote** keyword.

To log VPDN user events or VPDN tunnel-drop events to the syslog, you must configure the **vpdn logging** command with the **user** or the **tunnel-drop** keyword.

Configuring the **vpdn logging** command with the **accounting** keyword causes VPDN event log messages to be sent to a remote AAA server in a AAA vendor-specific attribute (VSA). This allows the correlation of VPDN call success rates with accounting records.

Note VPDN event logging to the syslog need not be enabled to allow the reporting of VPDN event log messages to a AAA server.

You can configure as many types of VPDN event logging as you want.

Examples

The following example enables VPDN logging locally:

```
vpdn logging local
```

The following example disables VPDN event logging locally, enables VPDN event logging at the remote tunnel endpoint, and enables the logging of both VPDN user and VPDN tunnel-drop events to the syslog of the remote router:

```
no vpdn logging local
vpdn logging remote
vpdn logging user
vpdn logging tunnel-drop
```

The following example disables the logging of VPDN events to the syslog both locally and at the remote tunnel endpoint, and enables the reporting of VPDN event log messages to the AAA server:

```
no vpdn logging local
no vpdn logging remote
vpdn logging accounting
```

Related Commands

Command	Description
vpdn history failure	Enables logging of VPDN failures to the history failure table or sets the failure history table size.

vpdn logging cause normal

To prevent display of the syslog message "VPDN-6-CLOSED" on the router console, use the **no vpdn logging cause normal** command in global configuration mode. To reenable display of the message (the default), use the **vpdn logging cause normal** command.

vpdn logging cause normal

no vpdn logging cause normal

Syntax Description

This command has no arguments or keywords.

Command Default

This command is enabled when VPDN logging is enabled, but it does not appear in the configuration of a Layer 2 access concentrator (LAC) or Layer 2 network server (LNS) when the running configuration is listed. When the **no** form of this commands is configured, it is listed in the running configuration. See the "Usage Guidelines" section for more information.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(5a)B1	This command was introduced.
12.3(11)T	This command was integrated into Cisco IOS Release 12.3(11)T.
12.3(4)T8	This command was integrated into Cisco IOS Release 12.3(4)T8.
12.3(7)T3	This command was integrated into Cisco IOS Release 12.3(7)T3.
12.3(8)T6	This command was integrated into Cisco IOS Release 12.3(7)T6.
12.3(7)XI3	This command was integrated into Cisco IOS Release 12.3(7)XI3.

Usage Guidelines

When users are declared as unauthenticated, their termination is recorded in the VPDN failure log. One method for determining why a subscriber cannot establish a PPP session is for the network operator to check the VPDN failure log for connection failure messages. The router can determine and log specific reasons for session termination, such as authentication failure, exceeding the session limit, timer expiration, and so on. However, a peer LAC or LNS sends the message "VPDN-6-CLOSED" to the router for any type of session termination. All other messages at the console and in the failure log appear under abnormal termination at that router, and the message “The remote server closed the session" is also logged in the VPDN connection failure log. So the failure log, which has maximum of 50 messages, is filled with messages. Once the maximum message length is reached, new messages begin replacing old messages and information about the unauthenticated users is lost.

The **no vpdn logging cause normal** command disables all system logging (syslog) messages with the prefix "VPDN-6-CLOSED." The **no vpdn history failure cause normal** command is used to prevent the message “The remote server closed the session" from being added to the connection failure log.

Both commands are independent so that configuring the **no vpdn logging cause normal** command does not prevent the message “The remote server closed the session” from being logged. And conversely, configuring the **no vpdn history failure cause normal** command does not prevent the syslog message "VPDN-6-CLOSED" from appearing.

By default, the **vpdn logging cause normal** command is enabled only when VPDN logging is enabled, and does not appear in the **show running-config** command output. When configured, the command **no vpdn logging cause normal** is listed in the **show running-config** command output only when VPDN logging is enabled.

By default, the **vpdn history failure cause normal** command is enabled only when the VPDN failure log is enabled, and it does not appear in the **show running-config** command output. When configured, the command **no vpdn history failure cause normal** shows up only when the VPDN history log is enabled.

Regardless of whether the **no vpdn logging cause normal** and the **no vpdn history failure cause normal** commands are configured, all other syslog messages except those with prefix "VPDN-6-CLOSED" appear on the console, and the failure table logs all messages except "The remote server closed the session."

Examples

The default behavior of this command enables display of the syslog message "VPDN-6-CLOSED." The following example shows how to disable both the "VPDN-6-CLOSED" and "The remote server closed the session" messages so that the VPDN connection failure log maintains useful messages about session termination:

```
no vpdn logging cause normal
no vpdn history failure cause normal
```

Related Commands

Command	Description
vpdn history failure cause normal	Prevents the message "The remote server closed the session" from overwriting useful messages in the VPDN connection failure log.

vpdn multihop

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

vpdn multihop

no vpdn multihop

Syntax Description

This command has no arguments or keywords.

Command Default

Multihop is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.3(5)T	This command was introduced.
12.2(8)B	Support was added for dialed number identification service (DNIS)-based multihop capability.
12.2(13)T	Support was added for DNIS-based multihop capability.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB, including support for DNIS-based multihop capability.

Usage Guidelines

Use this command to enable multihop VPDN. Multihop VPDN allows packets to pass through multiple VPDN tunnels. Ordinarily, packets are not allowed to traverse more than one tunnel. With multihop enabled, a packet can traverse as many as four tunnels.

VPDN multihop allows a router configured as a tunnel switch to act as both a network access server (NAS) and a tunnel server, receiving packets from an incoming VPDN tunnel and sending them out over an outgoing VPDN tunnel.

A tunnel switch can terminate incoming VPDN tunnels from multiple devices, and initiate outgoing tunnels to one or more tunnel servers. The outgoing tunnel is selected using either a domain name, a remote tunnel name, or a DNIS number. The order in which these criteria are searched by the software is determined by the **vpdn search-order** command.

VPDN multihop must be enabled for a Multichassis Multilink PPP (MMP) stack group deployment to function when incoming calls traverse a VPDN tunnel. For more information on configuring multihop VPDN for MMP, refer to the *Cisco IOS VPDN Configuration Guide* .

Examples

The following example configures the NAS, tunnel switch, and tunnel server to establish a multihop VPDN tunnel using L2TP:

NAS Configuration

```
! Configure the NAS to initiate VPDN dial-in sessions to the tunnel switch
vpdn-group 1
 request-dialin
  protocol l2tp
  domain cisco.com
!
 initiate-to ip 172.22.66.25
 local name ISP-NAS
```

Tunnel Switch Configuration

```
!Enable multihop
vpdn multihop
!
! Configure the tunnel switch to use the multihop hostname in the authentication search.
 vpdn search-order multihop-hostname domain dnis
!
! Configure the tunnel switch to accept dial-in sessions from the NAS
vpdn-group tunnelin
 accept-dialin
  protocol l2tp
  virtual-template 1
!
 terminate-from hostname ISP-NAS
 local name ISP-Sw
!
! Configure the tunnel switch to initiate VPDN dial-in sessions to the tunnel server
vpdn-group tunnelout
 request-dialin
  protocol l2tp
  multihop-hostname ISP-NAS
!
 initiate-to ip 10.2.2.2
 local name ISP-Sw
```

Tunnel Server Configuration

```
! Configure the tunnel server to accept dial-in sessions from the NAS
vpdn-group 1
 accept-dialin
  protocol l2tp
  virtual-template 1
!
 terminate-from hostname ISP-Sw
 local name ENT-TS
```

The following example configures one member of a stack group and a NAS for dial-in L2F VPDN tunneling. Multihop VPDN must be enabled on each stack group member to allow calls to be forwarded to the bundle owner.

Tunnel Server A Configuration

```
!Enable multihop VPDN
```

```
vpdn multihop
!
!Configure the tunnel server to accept L2F tunnels from the NAS
vpdn-group group1
 accept-dialin
  protocol l2f
  virtual-template 1
  exit
 terminate-from 172.18.32.139
!
!Configure the tunnel server as a stack group member
username user1 password mypassword
sgbp group mystack
sgbp member tunnelserverb 10.1.1.2
sgbp member tunnelserverc 10.1.1.3
```

NAS Configuration

```
!Configure the NAS to initiate L2F tunnels
vpdn-group group1
 request-dialin
  protocol l2f
  domain cisco.com
!
!Configure the NAS with the IP address of each tunnel server in the stack group
 initiate-to ip 10.1.1.1
 initiate-to ip 10.1.1.2
 initiate-to ip 10.1.1.3
```

Related Commands

Command	Description
vpdn enable	Enables VPDN networking on the router and informs the router to look for tunnel definitions in a local database and on a remote authorization server (home gateway), if one is present.
vpdn search-order	Specifies how a NAS or tunnel switch is to perform VPDN tunnel authorization searches.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.

vpdn outgoing

The **vpdn outgoing** command is replaced by the **request-dialin** command. See the description of the **request-dialin** command for more information.

vpdn pmtu

To manually configure a range of allowed path maximum transmission unit (MTU) sizes for a Layer 2 Tunneling Protocol (L2TP) virtual private dialup network (VPDN), use the **vpdn pmtu** command in global configuration mode. To restore the default value, use the **no** form of this command.

vpdn pmtu {**maximum** *bytes* | **minimum** *bytes*}

no vpdn pmtu

Syntax Description

maximum *bytes*	Sets the maximum allowed size, in bytes, for the path MTU. The range is 68 to 65535 bytes.
minimum *bytes*	Sets the minimum allowed size, in bytes, for the path MTU. The range is 68 to 65535 bytes.

Command Default

No maximum or minimum path MTU size is defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(25)	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(27)SB.

Usage Guidelines

Use the **vpdn pmtu** command to prevent Denial of Service (DoS) attacks against L2TP VPDN deployments that are performing path MTU discovery (PMTUD). PMTUD for an L2TP VPDN is disabled by default. To enable PMTUD, use the **ip pmtu** command.

When PMTUD is enabled, VPDN deployments are vulnerable to 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.

When an Internet host is performing PMTUD, crafted code 4 ICMP messages can be used to set the path MTU to an impractically low value. This causes 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.

Use the **vpdn pmtu** command to configure a range of acceptable values for the path MTU when PMTUD is enabled. If the device receives a code 4 ICMP message that advertises a next-hop path MTU outside the configured size range, the device ignores the ICMP message and display this log message:

```
%VPDN-5-IGNOREICMPMTU Ignoring received ICMP Type 3 Code 4, due to pmtu min or max setting
```

For information on detecting a PMTUD attack on an L2TP VPDN deployment, see *Cisco Security Advisory Crafted ICMP Messages Can Cause Denial of Service*.

Cisco software releases that support the **ip pmtu** command but do not support the **vpdn pmtu** command are vulnerable to PMTUD attacks. To protect a device running a vulnerable version of software, issue the **no ip pmtu** command to disable PMTUD.

For a complete list of Cisco software rebuild releases that support the**vpdn pmtu** command, see *Cisco Security Advisory Crafted ICMP Messages Can Cause Denial of Service*.

Examples

The following example enables PMTUD for the VPDN group named mygroup and configures the device to accept 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 mygroup
Router(config-vpdn)# ip pmtu
!
Router(config)# vpdn pmtu maximum 1460
Router(config)# vpdn pmtu minimum 576
```

Related Commands

Command	Description
ip pmtu	Enables the discovery of the path MTU for Layer 2 traffic.

vpdn profile

To associate a virtual private dialup network (VPDN) profile with a customer profile, use the **vpdn profile** command in customer profile configuration mode. To remove a VPDN profile from a customer profile, use the **no** form of this command.

vpdn profile *name*

no vpdn profile *name*

Syntax Description

name	VPDN profile name.

Command Default

No default behavior or values.

Command Modes

Customer profile configuration

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

Use the **vpdn profile** command to associate a VPDN profile with a customer profile.

VPDN profiles can be used to combine session counting over multiple VPDN groups. This ability can be applied to customer profiles by configuring multiple VPDN groups under a VPDN profile and by associating the VPDN profile with the customer profile by using the**vpdn profile** command.

Examples

The following example shows how to create two VPDN groups, configure the VPDN groups under a VPDN profile named profile1, and then associates the VPDN profile with a customer profile named customer12:

```
Router(config)# vpdn-group 1
Router(config-vpdn)#
!
Router(config)# vpdn-group 2
Router(config-vpdn)#
!
Router(config)# resource-pool profile vpdn profile1
Router(config-vpdn-profile)# vpdn group 1
Router(config-vpdn-profile)# vpdn group 2
```

```
!
Router(config)# resource-pool profile customer customer12
Router(config-vpdn-customer)# vpdn profile profile1
```

Related Commands

Command	Description
resource-pool profile customer	Creates a customer profile.
resource-pool profile vpdn	Creates a VPDN profile and enters VPDN profile configuration mode.
vpdn group	Associates a VPDN group with a customer or VPDN profile.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.

vpdn redirect

To enable Layer 2 Tunneling Protocol (L2TP) redirect functionality, use the **vpdn redirect** command in global configuration mode. To disable L2TP redirect functionality, use the **no** form of this command.

vpdn redirect

no vpdn redirect

Syntax Description

This command has no arguments or keywords.

Command Default

L2TP redirect functionality is disabled so that current multihop forwarding behavior is preserved.

Command Modes

Global configuration (config)

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

Configuring this command on the L2TP network access server (NAS) enables the NAS to perform L2TP redirection by sending a new vendor-specific attribute-value (AV) pair to the L2TP tunnel server. Configuring this command on the stack group tunnel server allows the tunnel server to redirect a call by disconnecting it and requesting the NAS to redirect it. The Stack Group Bidding Protocol (SGBP) stack group tunnel servers must have this command enabled to receive redirected calls, or else they receive calls only through the usual multihop forwarding from the tunnel server that first took the call.

Examples

The following example enables the L2TP redirect feature on the NAS:

```
Router(config)# vpdn redirect
```

Related Commands

Command	Description
clear vpdn redirect	Clears the L2TP redirect counters shown in the output from the **show vpdn redirect** command.
show vpdn redirect	Displays statistics for L2TP redirects and forwards.
vpdn redirect attempts	Restricts the number of redirect attempts possible for an L2TP call on the NAS.
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.

vpdn redirect attempts

To restrict the number of redirect attempts possible for a given Layer 2 Tunneling Protocol (L2TP) call on the L2TP network access server (NAS), use the **vpdn redirect attempts** command in global configuration mode. To restore the default value, use the **no** form of this command.

vpdn redirect attempts *number-of-attempts*

no vpdn redirect attempts *number-of-attempts*

Syntax Description

number-of-attempts	Number of redirect attempts, ranging from 1 to 20.

Command Default

A maximum of three redirect attempts are allowed.

Command Modes

Global configuration (config)

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

The number of redirect attempts is by default always restricted to three even if this command is not explicitly configured. The only use of this command is to configure a redirect attempts value other than the default (which is always in effect).

Examples

The following example configures four redirect attempts:

```
Router(config)# vpdn redirect attempts 4
```

Related Commands

Command	Description
clear vpdn redirect	Clears the L2TP redirect counters shown in the output from the **show vpdn redirect** command.
show vpdn redirect	Displays statistics for L2TP redirects and forwards.
vpdn redirect	Enables L2TP redirect functionality.
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.

vpdn redirect identifier

To configure a virtual private dialup network (VPDN) redirect identifier to use for Layer 2 Tunneling Protocol (L2TP) call redirection on a stack group tunnel server, use the **vpdn redirect identifier** command in global configuration mode. To remove the name of the redirect identifier from the tunnel server, use the **no** form of this command.

vpdn redirect identifier *identifier-name*

no vpdn redirect identifier *identifier-name*

Syntax Description

identifier-name	Name of the redirect identifier to use for call redirection.

Command Default

No identifier name is configured.

Command Modes

Global configuration (config)

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

The **vpdn redirect identifier** command is configured on each of the stack group tunnel servers. To configure the name of the redirect identifier on the network access server (NAS), use the **redirect identifier** command in VPDN group configuration mode.

The NAS compares the configured redirect identifier with the one received from the stack group tunnel server to determine authorization information to redirect the call.

Configuring the redirect identifier is not necessary to perform redirects. If the redirect identifier is not configured, the NAS uses the redirect IP address to obtain authorization information to redirect the call. In that case, the IP address of the new redirected tunnel server must be present in the **initiate-to** command configuration of the VPDN group on the NAS.

The redirect identifier allows new stack group members to be added without the need to update the NAS configuration with their IP addresses. With the redirect identifier configured, a new stack group member can be added and given the same redirect identifier as the rest of the stack group.

If the authorization information for getting to the new redirected tunnel server is different, then you must configure the authorization information via RADIUS using tagged attributes:

```
Cisco:Cisco-Avpair = :0:"vpdn:vpdn-redirect-id=
identifier name
"
```

The NAS chooses the correct tagged parameters to get authorization information for the new redirected tunnel server by first trying to match the redirect identifier (if present) or else by matching the Tunnel-Server-Endpoint IP address.

Examples

The following example configures the redirect identifier named lns1 on a stack group tunnel server:

```
Router(config)# vpdn redirect identifier lns1
```

The following attribute-value (AV) pair configures the RADIUS server with the redirect identifier named lns1 for a tunnel server:

```
Cisco:Cisco-Avpair = :0:"vpdn:vpdn-redirect-id=lns1"
```

Related Commands

Command	Description
clear vpdn redirect	Clears the L2TP redirect counters shown in the output from the **show vpdn redirect** command.
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.
vpdn redirect source	Configures the public redirect IP address of an L2TP stack group tunnel server.

vpdn redirect source

To configure the public redirect IP address of a Layer 2 Tunneling Protocol (L2TP) stack group tunnel server, use the **vpdn redirect source** command in global configuration mode. To remove the public redirect IP address of a stack group tunnel server, use the **no** form of this command.

vpdn redirect source *redirect-ip-address*

no vpdn redirect source *redirect-ip-address*

Syntax Description

redirect-ip-address	Public redirect IP address for a stack group tunnel server.

Command Default

If the **vpdn redirect source** command is not configured, then the IP address used for Stack Group Bidding Protocol (SGBP) bidding itself is used as the redirect address (the public redirect address is then omitted in the bid response).

Command Modes

Global configuration (config)

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

On the network access server (NAS), this command has no effect.

Examples

The following example configures a public IP address as a redirect source:

```
Router(config)# vpdn redirect source 10.1.1.1
```

Related Commands

Command	Description
clear vpdn redirect	Clears the L2TP redirect counters shown in the output from the **show vpdn redirect** command.
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.
vpdn redirect identifier	Configures a VPDN redirect identifier to use for L2TP call redirection on a stack group tunnel server.

vpdn search-order

To specify how a network access server (NAS) or tunnel switch performs virtual private dialup network (VPDN) tunnel authorization searches, use the **vpdn search-order** command in global configuration mode. To restore the default search order, use the **no** form of this command.

vpdn search-order {**dnis** [**domain**] [**multihop-hostname**] | **domain** [**dnis**] [**multihop-hostname**] | **multihop-hostname** [**dnis**] [**domain**]}

no vpdn search-order

Syntax Description

dnis	Searches on the dialed number identification service (DNIS) number.
domain	Searches on the domain name.
multihop-hostname	Searches on the hostname or tunnel ID of the ingress tunnel for a multihop tunnel switch.

Command Default

When this command is disabled, by default the router searches first on the DNIS number provided on ISDN lines and then searches on the domain name. This is equivalent to issuing the **vpdn search-order dnis domain** command.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.3	This command was introduced.
12.2(13)T	The **multihop-hostname** keyword was added.
12.2(28)SB	The **multihop-hostname** keyword was added.

Usage Guidelines

To issue the **vpdn search-order** command, you must include at least one of the search parameter keywords. You can enter multiple keywords, and they can be entered in any order. The order of the keywords specifies the order of precedence given to the search parameters. If you do not issue a particular keyword, no search is performed on that parameter.

Issue the **multihop-hostname** keyword only on a device configured as a multihop tunnel switch.

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

Examples

The following example configures a NAS to perform tunnel authorization searches based on DNIS number only:

```
vpdn search-order dnis
```

The following example configures a tunnel switch to select a tunnel destination based on the multihop hostname first, then on the domain name, and finally on the DNIS number:

```
vpdn search-order multihop-hostname domain dnis
```

Related Commands

Command	Description
multihop-hostname	Enables the tunnel switch to initiate a tunnel based on the hostname or tunnel ID of the ingress tunnel.
vpdn multihop	Enables VPDN multihop.

vpdn session accounting

To enable tunnel-link type accounting records to be sent to the RADIUS server, use the **vpdn session accounting** command in global configuration mode. To disable the tunnel-link type accounting records, use the **no** form of this command.

vpdn session accounting {**network** *list-name* | **suppress multihop** {**inbound** | **outbound**}}

no vpdn session accounting {**network** | **suppress**}

Syntax Description

network	Specifies the virtual private dialup network (VPDN) network session accounting method.
list-name	Character string used to name the list of at least one accounting method. The *list-name* value specified in this command must match the *list-name* value defined in the **aaa accounting** command; otherwise, network accounting does not occur.
suppress	Suppresses the accounting options in the VPDN network session.
multihop	Suppresses the multihop attributes in the VPDN network session.
inbound	Suppresses the multihop inbound tunnel attributes in the VPDN network session.
outbound	Suppresses the multihop outbound tunnel attributes in the VPDN network session.

Command Default

Tunnel-link type accounting records are not sent.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(15)B	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Release	Modification
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
15.0(1)M	This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The **inbound**, **multihop**, **outbound**, and the **suppress** keywords were added.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

Before you enable the **vpdn session accounting network** command, you must enable network accounting by using the **aaa accounting** command.

Note If the default network accounting method list is configured and no additional accounting configurations are enabled on the interface, network accounting is enabled by default. If the **vpdn session accounting network** command is linked to the default method list, all tunnel-link accounting records are enabled for those sessions.

This command displays the following tunnel-link accounting type records, which are used with the RADIUS accounting attribute Acct-Status-Type (attribute 40):

- Tunnel-Link-Start (12)--Marks the creation of a tunnel link.
- Tunnel-Link-Stop (13)--Marks the end of a tunnel link.

Note Only some tunnel types (such as Layer 2 Tunneling Protocol [L2TP]) support the multiple links per tunnel; these values should be included for accounting packets for tunnel types that support multiple links per tunnel.

- Tunnel-Link-Reject (14)--Marks the rejection of a tunnel setup for a new link in an existing tunnel. Only some tunnel types (L2TP) support the multiple links per tunnel; this value should be included only in accounting packets for tunnel types that support multiple links per tunnel.

Note If either Tunnel-Link-Start or Tunnel-Link-Stop is enabled, Tunnel-Link-Reject is sent even if it has not been enabled.

Examples

The following example shows how to configure an L2TP access concentrator (LAC) to send tunnel-link type accounting records to the RADIUS server:

```
aaa accounting network m1 start-stop group radius
vpdn enable
vpdn tunnel accounting network m1
vpdn session accounting network m1
vpdn search-order domain dnis
!
vpdn-group 1
 request-dialin
  protocol l2tp
  domain cisco.com
 initiate-to ip 10.1.1.1
 local name ISP_LAC
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+.
vpdn tunnel accounting network	Enables tunnel type accounting records to be sent to the RADIUS server.

vpdn session-limit

To limit the number of simultaneous virtual private dialup network (VPDN) sessions allowed on a router, use the **vpdn session-limit** command in global configuration mode. To remove a configured session limit restriction, use the **no** form of this command.

vpdn session-limit *sessions*

no vpdn session-limit

Syntax Description

sessions	Maximum number of simultaneous VPDN sessions that are allowed on a router. The range is 1 to 5000.

Command Default

No session limit exists for the router.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(6)T	This command was introduced.

Usage Guidelines

Use the **vpdn session-limit** command to configure the maximum number of VPDN sessions allowed on the router.

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 sets a limit of two simultaneous VPDN sessions on the router:

```
vpdn session-limit 2
```

Related Commands

Command	Description
group session-limit	Limits the number of simultaneous VPDN sessions allowed across all VPDN groups associated with a particular VPDN template.
show vpdn session	Displays session information about active Layer 2 sessions for a VPDN.
session-limit (VPDN)	Limits the number of simultaneous VPDN sessions allowed for a specified VPDN group.

vpdn softshut

To prevent new sessions from being established on a virtual private dialup networking (VPDN) tunnel without disturbing existing sessions, use the **vpdn softshut** command in global configuration mode. To return VPDN tunnels to active service, use the **no** form of this command.

vpdn softshut

no vpdn softshut

Syntax Description

This command has no arguments or keywords.

Command Default

New sessions can be established.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

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

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

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

Examples

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

```
Router(config)# vpdn softshut
Router(config)#
00:11:17:%VPDN-6-SOFTSHUT:L2F HGW great_went has turned on softshut and rejected user
user1@cisco.com
Router(config)#
```

Related Commands

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

vpdn source-ip

To globally specify an IP address that is different from the physical IP address used to open a virtual private dialup network (VPDN) tunnel, use the **vpdn source-ip** command in global configuration mode. To disable use of the alternate IP address, use the **no** form of this command.

vpdn source-ip *ip-address*

no vpdn source-ip *ip-address*

Syntax Description

ip-address	Alternate IP address.

Command Default

No alternate IP address is specified.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

Use the **vpdn source-ip** command to specify a single alternate IP address to be used for all tunnels on the device. A single source IP address can be configured globally per device.

Use the **source-ip** command in VPDN group configuration mode to configure an alternate IP address to be used for only those tunnels associated with that VPDN group.

The VPDN group-level configuration overrides the global configuration.

Examples

This example sets a source IP address of 172.24.48.3:

```
vpdn source-ip 172.24.48.3
```

Related Commands

Command	Description
source-ip	Specifies an IP address that is different from the physical IP address used to open a VPDN tunnel for the tunnels associated with a VPDN group.

Command	Description
vpdn enable	Enables VPDN on the router and informs the router to look for tunnel definitions in a local database and on a remote authorization server, if one is present.

vpdn tunnel accounting network

To enable tunnel type accounting records to be sent to the RADIUS server, use the **vpdn tunnel accounting network** command in global configuration mode. To disable tunnel type accounting records, use the **no** form of this command.

vpdn tunnel accounting network *list-name*

no vpdn tunnel accounting network *list-name*

Syntax Description

list-name	Character string used to name the list of at least one accounting method. The *list-name* value must match the *list-name* value defined in the **aaa accounting** command; otherwise, network accounting does not occur.

Command Default

Tunnel type accounting records are not sent.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(15)B	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

Before you enable the **vpdn tunnel accounting network** command, you must enable network accounting by using the **aaa accounting** command.

Note If the default network accounting method list is configured and no additional accounting configurations are enabled on the interface, network accounting is enabled by default. If the **vpdn tunnel accounting network** command is linked to the default method list, all tunnel accounting records are enabled for those sessions.

This command displays the following tunnel accounting type records, which are used with the RADIUS accounting attribute Acct-Status-Type (attribute 40):

- Tunnel-Start (9)--Marks the beginning of a tunnel setup with another node.
- Tunnel-Stop (10)--Marks the end of a tunnel connection to or from another node.
- Tunnel-Reject (11)--Marks the rejection of a tunnel setup with another node.

Note If either Tunnel-Start or Tunnel-Stop are enabled, Tunnel-Reject is sent even if it has not been enabled.

Examples

The following example shows how to configure an L2TP access concentrator (LAC) to send tunnel type accounting records to the RADIUS server:

```
! The method list defined in the VPDN command must be the same as the method list
defined ! in aaa accounting command; otherwise, accounting will not occur.
aaa accounting network m1 start-stop group radius
vpdn enable
vpdn tunnel accounting network m1
vpdn session accounting network m1
vpdn search-order domain dnis
!
vpdn-group 1
 request-dialin
  protocol l2tp
  domain cisco.com
 initiate-to ip 10.1.1.1
 local name ISP_LAC
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+.
vpdn session accounting network	Enables tunnel-link type accounting records to be sent to the RADIUS server.

vpdn tunnel authorization network

To enable the Layer 2 Tunnel Protocol (L2TP) tunnel server or network access server (NAS) to perform remote authentication, authorization, and accounting (AAA) tunnel authentication and authorization, use the **vpdn tunnel authorization network** command in global configuration mode. To disable remote tunnel authentication and authorization and return to the default setting, use the **no** form of this command.

vpdn tunnel authorization network {*list-name* | **default**}

no vpdn tunnel authorization network {*list-name* | **default**}

Syntax Description

list-name	Character string used to name the list of at least one accounting method. If the *list-name* argument was specified in the **aaa authorization network** command, you must use the same list name with the **vpdn tunnel authorization network** command.
default	Specifies the default authorization methods that are listed with the **aaa authorization network** command. If the **default** keyword was specified in the **aaa authorization network** command, you must use the **default** keyword with the **vpdn tunnel authorization network** command.

Command Default

If this command is not enabled, the device performs authentication locally.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(15)B	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

Use this command to specify the authorization method list that is used for remote tunnel hostname-based authorization. The method list (named or default) is defined using the **aaa authorization network** command.

If a method list for tunnel authorization is not specified via the **aaa authorization network** command, local authorization using the local virtual private dialup network (VPDN) group configuration occurs.

Note This method list is only for L2TP tunnel authorization and termination; it is not intended for domain or dialed number identification service (DNIS)-based authorization that is typically done on the tunnel terminator. Thus, this command can be enabled only on the tunnel terminator--the NAS for dial-out and the tunnel server for dial-in.

Examples

The following example shows how to configure the tunnel server to enable remote RADIUS tunnel authentication and authorization:

```
! Define a RADIUS server group
Router(config)# aaa group server radius VPDN-group

Router(config-sg-radius)# server 10.102.48.91 auth-port 1645 acct-port 1646
Router(config-sg-radius)# exit
Router(config)# aaa authorization network mymethodlist group VPDN-Group

Router(config)# vpdn tunnel authorization network mymethodlist
Router(config)# vpdn tunnel authorization virtual-template 10
```

Related Commands

Command	Description
aaa authorization	Sets parameters that restrict user access to a network.

vpdn tunnel authorization password

To configure a password for the RADIUS authentication request to retrieve the tunnel configuration that is based on the remote tunnel hostname, use the **vpdn tunnel authorization password** command in global configuration mode. To return to the default password, use the **no** form of this command.

vpdn tunnel authorization password *password*

no vpdn tunnel authorization password *password*

Syntax Description

password	Character string, which is truncated after 25 characters.

Command Default

The password is set to "cisco."

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(15)B	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

This command can be used on either the Layer 2 Tunneling Protocol (L2TP) network access server (NAS) or on the L2TP tunnel server when remote RADIUS tunnel authentication is enabled.

Examples

The following example shows how to set the password to configure the tunnel server to enable remote RADIUS tunnel authentication and authorization and how to set the password to mypassword:

```
Router(config)# aaa authorization network mymethodlist group VPDN-Group

Router(config)# vpdn tunnel authorization network mymethodlist
Router(config)# vpdn tunnel authorization virtual-template 10
Router(config)# vpdn tunnel authorization password mypassword
```

Related Commands

Command	Description
vpdn tunnel authorization network	Enables the L2TP tunnel server or NAS to perform remote AAA tunnel authentication and authorization.

vpdn tunnel authorization virtual-template

To select the default virtual template from which to clone virtual access interfaces, use the **vpdn tunnel authorization virtual-template** command in global configuration mode. To remove the default virtual template, use the **no** form of this command.

vpdn tunnel authorization virtual-template *vtemplate-number*

no vpdn tunnel authorization virtual-template *vtemplate-number*

Syntax Description

vtemplate-number	The default virtual template number that is used for cloning on the local router. The range is 1 to 200.

Command Default

No default virtual template is specified.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(15)B	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

This command should be used if a virtual template is not specified in the local virtual private dialup network (VPDN) group (for local authentication) or in a remote RADIUS configuration (via the vpdn-vtemplate attribute).

Note This command applies only on the L2TP tunnel server.

Examples

The following example shows how to configure the tunnel server to enable remote RADIUS tunnel authentication and authorization and how to specify a default virtual template:

```
! Define a RADIUS server group
```

```
Router(config)# aaa group server radius VPDN-group

Router(config-sg-radius)# server 10.102.48.91 auth-port 1645 acct-port 1646
Router(config-sg-radius)# exit
! RADIUS configurations only
Router(config)# aaa authorization network mymethodlist group VPDN-Group

Router(config)# vpdn tunnel authorization network mymethodlist
! Can be used for local vpdn-group tunnel authentication or remote RADIUS tunnel
! authentication
Router(config)# vpdn tunnel authorization virtual-template 10
```

Related Commands

Command	Description
vpdn tunnel authorization network	Enables the L2TP tunnel server or NAS to perform remote AAA tunnel authentication and authorization.

vpdn-group

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

vpdn-group *name*

no vpdn-group *name*

Syntax Description

name	Name of the VPDN group.

Command Default

VPDN groups are not created.

Command Modes

Global configuration (config)

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.
12.2(33)SB	This command's behavior was modified and implemented on the Cisco 10000 series router as described in the Usage Guidelines section.
Cisco IOS XE Release 3.3S	This command was modified. The message for duplicate configurations was enhanced to include more information as described in the Usage Guidelines section.

Usage Guidelines

Use the **vpdn-group** command to configure VPDN parameters that are always applied to that VPDN group. System default settings for VPDN parameters are applied for any settings not configured in the individual VPDN group or in the associated VPDN template.

VPDN groups are associated with the global VPDN template by default. You can associate individual VPDN groups with a named VPDN template instead. Associating a VPDN group with a named VPDN template disassociates the VPDN group from the global VPDN template.

If you create two VPDN groups with the same configuration, this message displays:

```
% Warning, the vpdn groups group1 and group2 have the same configuration
```

You should change one of the group configurations to eliminate the duplicate configuration. Leaving the duplicate configurations in place can lead to unexpected (and unsupported) results.

Cisco 10000 Series Usage Guidelines

In Cisco IOS Release 12.2(33)SB and later releases, the router does not accept the **vpdn-group** command if you issue the command before you issue the **vpdn enable** command. Instead, this message displays:

```
% VPDN configuration is not allowed until VPDN is enabled through 'vpdn enable'.
```

In releases prior to Cisco IOS Release 12.2(33)SB, if you issue the **vpdn-group** command before the **vpdn enable** command, the router accepts the command and displays this message:

```
% VPDN is not enabled
```

Examples

The following example configures a source IP address for tunnels associated with the VPDN group named tunneling. This source IP address overrides any configured global source IP address for tunnels associated with this VPDN group.

```
Router(config)# vpdn enable
Router(config)# vpdn-group tunneling
Router(config-vpdn)# source-ip 10.1.1.2
```

The following example configures two VPDN parameters in a VPDN template named l2tp. The named VPDN template is associated with the VPDN group named l2tp_tunnels.

```
Router(config)# vpdn enable
Router(config)# vpdn-template l2tp
Router(config-vpdn-templ)# l2tp tunnel busy timeout 65
Router(config-vpdn-templ)# l2tp tunnel password tunnel4me
Router(config-vpdn-templ)# exit
Router(config)# vpdn-group l2tp_tunnels
Router(config-vpdn)# source vpdn-template l2tp_tunnels
Router(config-vpdn-profile)# vpdn group yourgroup
```

Related Commands

Command	Description
vpdn enable	Enables VPDN on the router and directs the router to look for tunnel definitions in a local database and on a remote authorization server (home gateway), if one is present.
vpdn-template	Creates a VPDN template and enters VPDN template configuration mode.
vpdn profile	Associates a VPDN profile with a customer profile.

vpdn-template

To create a virtual private dialup network (VPDN) template and enter VPDN template configuration mode, use the **vpdn-template** command in global configuration mode. To delete a VPDN template, use the **no** form of this command.

vpdn-template [*name*]

no vpdn-template [*name*]

Syntax Description

name	(Optional) Name of a VPDN template.

Command Default

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

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(4)B	This command was introduced on the Cisco 7200 series and Cisco 7401ASR routers.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T without support for the *name* argument.
12.2(13)T	The *name* argument was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

Use this command to configure values for VPDN parameters in a VPDN template. A single unnamed VPDN template can be configured. Multiple named VPDN templates can be configured. A VPDN group can be associated with only one VPDN template.

Values configured in the global (unnamed) VPDN template are applied to all VPDN groups by default. A VPDN group can be disassociated from the global VPDN template, or associated with a named VPDN template. Associating a VPDN group with a named VPDN template automatically disassociates it from the global VPDN template.

The values configured in a VPDN template are applied to all associated VPDN groups unless specific values are configured for individual VPDN groups. VPDN parameters that are not specified in the individual VPDN group or in the associated VPDN template are assigned system default values.

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

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

Not all commands that are available for configuring a VPDN group can be used to configure a VPDN template. The table below lists the commands that can be used to configure the VPDN template.

Table 33 Commands Available for VPDN Template Configuration

Command Name	Description
default (VPDN)	Removes a VPDN subgroup configuration, or resets it to its default value.
description	Adds a description for a VPDN group.
group session-limit	Specifies the maximum number of concurrent sessions allowed across all VPDN groups associated with a particular VPDN template.
ip mtu adjust	Enables automatic adjustment of the IP maximum transmission unit (MTU) on a virtual access interface.
ip pmtu	Enables the discovery of the path MTU for Layer 2 traffic.
ip precedence (VPDN)	Sets the precedence value in the VPDN Layer 2 encapsulation header.
ip tos (VPDN)	Sets the type of service (ToS) bits in the VPDN Layer 2 encapsulation header.
l2f ignore-mid-sequence	Configures the router to ignore message identifier (MID) sequence numbers for sessions in a Layer 2 Forwarding (L2F) tunnel.
l2f tunnel busy timeout	Configures the amount of time that the router waits before attempting to recontact an L2F peer that was previously busy.
l2f tunnel retransmit initial retries	Configures the number of times that the router attempts to send the initial control packet for tunnel establishment before considering an L2F peer busy.
l2f tunnel retransmit retries	Configures the number of times the router attempts to resend an L2F tunnel control packet before tearing the tunnel down.

Command Name	Description
l2f tunnel timeout setup	Configures the amount of time that the router waits for a confirmation message after sending out the initial L2F control packet before considering a peer busy.
l2tp attribute clid mask-method	Configures a network access server (NAS) to provide Layer 2 Tunnel Protocol (L2TP) calling line ID suppression for local authorization.
l2tp drop out-of-order	Instructs a NAS or tunnel server using L2TP to drop packets that are received out of order.
l2tp hidden	Enables L2TP attribute-value (AV) pair hiding, which encrypts the value of sensitive AV pairs.
l2tp ip udp checksum	Enables IP User Datagram Protocol (UDP) checksums on L2TP payload packets.
l2tp security crypto-profile	Configures IP Security (IPSec) protection of L2TP sessions associated with a VPDN group.
l2tp sequencing	Enables sequencing for packets sent over an L2TP tunnel.
l2tp tunnel authentication	Enables L2TP tunnel authentication.
l2tp tunnel bearer capabilities	Sets the bearer-capability value used by the Cisco router.
l2tp tunnel busy timeout	Configures the amount of time that the router waits before attempting to recontact an L2TP peer that was previously busy.
l2tp tunnel framing capabilities	Sets the framing-capability value used by the Cisco router.
l2tp tunnel hello	Sets the number of seconds between sending hello keepalive packets for an L2TP tunnel.
l2tp tunnel password	Sets the password the router uses to authenticate the tunnel.
l2tp tunnel receive-window	Configures the number of packets allowed in the local receive window for an L2TP control channel.
l2tp tunnel retransmit initial retries	Configures the number of times that the router attempts to send out the initial L2TP control packet for tunnel establishment before considering a peer busy.

Command Name	Description
l2tp tunnel retransmit initial timeout	Configures the amount of time that the router waits before resending an initial L2TP control packet to establish a tunnel.
l2tp tunnel retransmit retries	Configures the number of retransmission attempts made for an L2TP control packet.
l2tp tunnel retransmit timeout	Configures the amount of time that the router waits before resending an L2TP control packet.
l2tp tunnel timeout no-session	Configures the time a router waits after an L2TP tunnel becomes empty before tearing down the tunnel.
l2tp tunnel timeout setup	Configures the amount of time that the router waits for a confirmation message after sending the initial L2TP control packet before considering a peer busy.
l2tp tunnel zlb delay	Configures the delay time before a zero length bit (ZLB) control message must be acknowledged.
local name	Specifies a local hostname that the tunnel uses to identify itself.
pptp flow-control receive-window	Specifies how many packets the Point-to-Point Tunnel Protocol (PPTP) client can send before it must wait for the acknowledgment from the tunnel server.
pptp flow-control static-rtt	Specifies the timeout interval of the PPTP tunnel server between sending a packet to the client and receiving a response.
pptp tunnel echo	Specifies the period of idle time on the PPTP tunnel that triggers an echo message from the tunnel server to the client.
redirect identifier	Configures a VPDN redirect identifier to use for L2TP call redirection on a NAS.
relay pppoe bba-group	Configures the PPP over Ethernet (PPPoE) broadband access (BBA) group that responds to PPPoE Active Discovery (PAD) messages.
vpn	Specifies that the source and destination IP addresses of a given VPDN group belong to a specified VPN routing and forwarding instance (VRF).

Examples

The following example enters VPDN template configuration mode and configures two VPDN parameters in the global VPDN template:

```
Router(config)# vpdn-template
Router(config-vpdn-templ)# local name myrouter
Router(config-vpdn-templ)# ip mtu adjust
```

The following example creates a VPDN template named l2tp, enters VPDN template configuration mode, configures two VPDN parameters in the VPDN template, and associates the VPDN group named l2tptunnels with the VPDN template:

```
Router(config)# vpdn-template l2tp
Router(config-vpdn-templ)# l2tp tunnel busy timeout 65
Router(config-vpdn-templ)# l2tp tunnel password 7 tunnel4me
!
Router(config)# vpdn-group l2tptunnels
Router(config-vpdn)# source vpdn-template l2tp
```

The following example configures a VPDN template called customer1 and applies a group session limit of 50 to all VPDN groups associated with that VPDN template:

```
Router(config)# vpdn-template customer1
Router(config-vpdn-templ)# group session-limit 50
```

Related Commands

Command	Description
group session-limit	Specifies the maximum number of concurrent sessions allowed across all VPDN groups associated with a particular VPDN template.
source vpdn-template	Associates a VPDN group with a VPDN template.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.

vpn

To specify that the source and destination IPv4 addresses of a given virtual private dialup network (VPDN) group belong to a specified virtual private network (VPN) routing and forwarding (VRF) instance, use the **vpn** command in VPDN group or VPDN template configuration mode. To disassociate all IPv4 addresses in a VPDN group from a VRF, use the **no** form of this command.

vpn {**vrf** *vrf-name* | **id** *vpn-id*}

no vpn

Syntax Description

vrf *vrf-name*	Name of the VRF instance to be associated with the IPv4 addresses of the VPDN group.
id *vpn-id*	VPN ID of the VRF to be associated with the IPv4 addresses of the VPDN group.

Command Default

VPDN groups are not associated with a VRF.

Command Modes

VPDN group configuration (config-vpdn)

VPDN template configuration (config-vpdn-temp)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.3(7)XI7	This command was integrated into Cisco IOS Release 12.3(7)XI7 and implemented on the Cisco 10000 series routers.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB for the PRE2.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was implemented on the Cisco 10000 series router for the PRE3.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

Use the **vpn** command to configure the software to look up a VPDN source or destination IPv4 address in a specific VPN routing table instead of the global routing table.

Before you can issue the **vpn** command, a VRF instance must be created by using the **ip vrf** command.

The **vpn** command can be used with both dial-in and dial-out VPDN scenarios.

Examples

The following example associates the IP addresses configured in the VPDN group named group1 with the VRF named vrf-second:

```
vpdn-group group1
 request-dialin
 protocol l2tp
!
 vpn vrf vrf-second
 source-ip 172.16.1.9
 initiate-to ip 172.16.1.1
```

The following example associates the IP addresses configured in the VPDN group named group2 with the VPN ID 11:2222:

```
vpdn-group group2
 request-dialin
 protocol l2tp
!
 vpn id 11:2222
 source-ip 172.16.1.9
 initiate-to ip 172.16.1.1
```

Related Commands

Command	Description
ip vrf	Configures a VRF routing table.
show ip route	Displays all static IP routes, or those installed using the AAA route download function.
show vpdn session	Displays session information about active Layer 2 sessions for a VPDN.
show vpdn tunnel	Displays information about active Layer 2 tunnels for a 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.