M through T

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

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 1 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 2 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 3 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 4 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 5 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 6 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 7 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 8 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 9 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 10 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 11 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 12 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 13 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 14 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 15 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 16 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 17 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 18 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 19 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 20 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 21 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 22 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 23 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 24 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 25 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 26 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