L

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

l2f ignore-mid-sequence

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

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

l2f ignore-mid-sequence

no l2f ignore-mid-sequence

Syntax Description

This command has no arguments or keywords.

Command Default

MID sequence numbers are not ignored.

Command Modes

VPDN group configuration (config-vpdn)

VPDN template configuration (config-vpdn-temp)

Command History

Release	Modification
11.3(5)AA	This command was introduced.
12.0(1)T	This command was integrated into Cisco IOS Release 12.0(1)T.
12.4(11)T	This command has been removed.

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

l2f tunnel busy timeout

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

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

l2f tunnel busy timeout *seconds*

no l2f tunnel busy timeout

Syntax Description

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

Command Default

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

Command Modes

VPDN group configuration (config-vpdn)

VPDN template configuration (config-vpdn-temp)

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(11)T	This command was implemented on the Cisco 1760, Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.4(11)T	This command was removed.

Examples

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

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

Related Commands

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

l2f tunnel retransmit initial retries

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

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

l2f tunnel retransmit initial retries *number*

no l2f tunnel retransmit initial retries

Syntax Description

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

Command Default

The router sends the initial control packet twice.

Command Modes

VPDN group configuration (config-vpdn)

VPDN template configuration (config-vpdn-temp)

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(11)T	This command was implemented on the Cisco 1760, Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.4(11)T	This command was removed.

Usage Guidelines

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

Examples

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

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

Related Commands

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

l2f tunnel retransmit retries

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

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

l2f tunnel retransmit retries *number*

no l2f tunnel retransmit retries

Syntax Description

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

Command Default

The router resends control packets six times.

Command Modes

VPDN group configuration (config-vpdn)

VPDN template configuration (config-vpdn-temp)

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(11)T	This command was implemented on the Cisco 1760, Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.4(11)T	This command was removed.

Usage Guidelines

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

Examples

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

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

Related Commands

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

l2f tunnel timeout setup

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

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

l2f tunnel timeout setup *seconds*

no l2f tunnel timeout setup

Syntax Description

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

Command Default

The router waits 10 seconds for a confirmation message.

Command Modes

VPDN group configuration (config-vpdn)

VPDN template configuration (config-vpdn-temp)

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(11)T	This command was implemented on the Cisco 1760, Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.4(11)T	This command was removed.

Usage Guidelines

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

Examples

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

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

Related Commands

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

l2tp attribute clid mask-method

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

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

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

Syntax Description

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

Command Default

The calling station ID is not masked or dropped.

Command Modes

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

Command History

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

Usage Guidelines

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

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

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

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

Examples

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

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

Related Commands

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

l2tp congestion-control

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

l2tp congestion-control

no l2tp congestion-control

Syntax Description

This command has no arguments or keywords.

Command Default

L2TP congestion avoidance is enabled.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

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

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

Examples

The following example enables L2TP congestion avoidance:

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

Related Commands

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

l2tp drop out-of-order

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

l2tp drop out-of-order

no l2tp drop out-of-order

Syntax Description

This command has no arguments or keywords.

Command Default

Out of order packets are not dropped.

Command Modes

VPDN group configuration (config-vpdn)

VPDN template configuration (config-vpdn-temp)

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

l2tp hidden

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

l2tp hidden

no l2tp hidden

Syntax Description

This command has no arguments or keywords.

Command Default

L2TP AV pair hiding is disabled.

Command Modes

VPDN group configuration (config-vpdn)

VPDN template configuration (config-vpdn-temp)

Command History

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

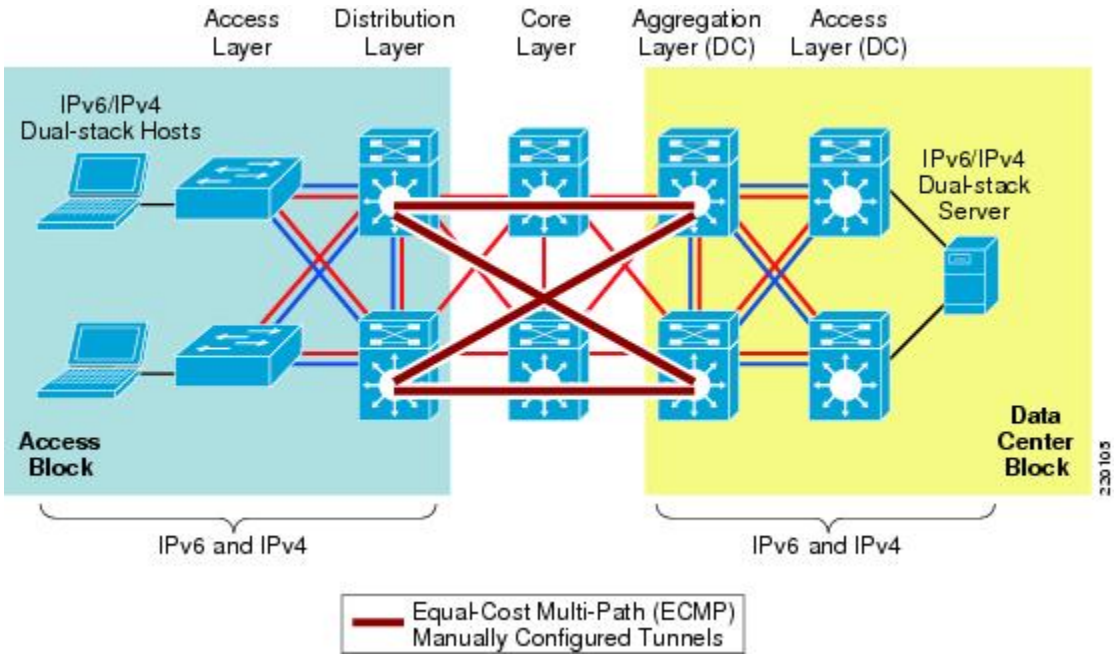
Usage Guidelines

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

In the figure below, the client initiates a PPP session with the LAC, and tunnel authentication begins. The LAC in turn exchanges authentication requests with the LNS. Upon successful authentication between the LAC and LNS, a tunnel is created. Proxy authentication is performed by the LAC using either PAP or Challenge Handshake Authentication Protocol (CHAP). Because PAP username and password information

is exchanged between devices in clear-text, use the **l2tp hidden** command where L2TP AV pair values are encrypted.

Figure 1 LAC-LNS Proxy Authentication



Examples

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

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

Related Commands

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

l2tp ip udp checksum

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

l2tp ip udp checksum

no l2tp ip udp checksum

Syntax Description

This command has no arguments or keywords.

Command Default

UDP checksums are not used on L2TP data packets.

Command Modes

VPDN group configuration (config-vpdn)

VPDN template configuration (config-vpdn-temp)

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

l2tp rx-speed

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

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

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

Syntax Description

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

Command Default

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

Command Modes

VPDN group configuration (config-vpdn)

VPDN template configuration (config-vpdn-temp)

Command History

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

Usage Guidelines

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

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

Examples

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

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

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

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

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

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

Related Commands

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

l2tp security crypto-profile

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

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

no l2tp security crypto-profile

Syntax Description

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

Command Default

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

Command Modes

VPDN group configuration (config-vpdn)

VPDN template configuration (config-vpdn-temp)

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

Related Commands

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

l2tp security ip address-check

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

l2tp security ip address-check

no l2tp security ip address-check

Syntax Description

This command has no arguments or keywords.

Command Default

The command is disabled.

Command Modes

VPDN-group configuration (config-vpdn)

Command History

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

Usage Guidelines

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

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

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

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

Examples

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

```
LAC> enable

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

Related Commands

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

l2tp sequencing

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

l2tp sequencing

no l2tp sequencing

Syntax Description

This command has no arguments or keywords.

Command Default

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

Command Modes

VPDN group configuration (config-vpdn)

VPDN template configuration (config-vpdn-temp)

Command History

Release	Modification
12.1	This command was introduced.

Usage Guidelines

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

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

Tunnel Initiator

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

Tunnel Terminator

- By default, sequence numbers are off.

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

Examples

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

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

Related Commands

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

l2tp sso enable

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

l2tp sso enable

no l2tp sso enable

Syntax Description

This command has no arguments or keywords.

Command Default

L2TP SSO is enabled.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

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

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

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

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

Examples

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

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

Related Commands

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

l2tp tunnel authentication

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

l2tp tunnel authentication

no l2tp tunnel authentication

Syntax Description

This command has no arguments or keywords.

Command Default

L2TP tunnel authentication is enabled.

Command Modes

VPDN group configuration (config-vpdn)

VPDN template configuration (config-vpdn-temp)

Command History

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

Examples

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

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

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

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

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

Related Commands

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

l2tp tunnel bearer capabilities

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

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

no l2tp tunnel bearer capabilities

Syntax Description

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

Command Default

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

Command Modes

VPDN group configuration (config-vpdn)

VPDN template configuration (config-vpdn-temp)

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

l2tp tunnel busy timeout

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

l2tp tunnel busy timeout *seconds*

no l2tp tunnel busy timeout

Syntax Description

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

Command Default

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

Command Modes

VPDN group configuration (config-vpdn)

VPDN template configuration (config-vpdn-temp)

Command History

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

Examples

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

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

Related Commands

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

l2tp tunnel framing capabilities

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

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

no l2tp tunnel framing capabilities

Syntax Description

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

Command Default

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

Command Modes

VPDN group configuration (config-vpdn)

VPDN template configuration (config-vpdn-temp)

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

l2tp tunnel hello

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

l2tp tunnel hello *seconds*
no l2tp tunnel hello

Syntax Description

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

Command Default

Hello keepalive packets are sent every 60 seconds.

Command Modes

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

Command History

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

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

l2tp tunnel password

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

l2tp tunnel password *password*

no l2tp tunnel password

Syntax Description

password	String that the router uses for tunnel authentication.

Command Default

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

Command Modes

VPDN group configuration (config-vpdn)

VPDN template configuration (config-vpdn-temp)

Command History

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

Usage Guidelines

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

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

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

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

Examples

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

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

Related Commands

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

l2tp tunnel receive-window

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

l2tp tunnel receive-window *packets*

no l2tp tunnel receive-window

Syntax Description

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

Command Default

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

Command Modes

VPDN group configuration (config-vpdn)

VPDN template configuration (config-vpdn-temp)

Command History

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

Usage Guidelines

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

Cisco 10000 Series Router

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

Examples

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

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

Related Commands

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

l2tp tunnel resync

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

l2tp tunnel resync *packets*

no l2tp tunnel resync

Syntax Description

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

Command Default

This command is disabled

Command Modes

VPDN group configuration (config-vpdn)

Command History

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

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

l2tp tunnel retransmit initial retries

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

l2tp tunnel retransmit initial retries *number*
no l2tp tunnel retransmit initial retries

Syntax Description

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

Command Default

The router resends the initial L2TP control packet twice.

Command Modes

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

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

Command	Description
l2tp tunnel busy timeout	Configures the amount of time that the router waits before attempting to recontact a router that was previously busy.
l2tp tunnel retransmit initial timeout	Configures the amount of time that the router waits before resending an initial L2TP control packet out to establish a tunnel.
l2tp tunnel retransmit retries	Configures the number of retransmission attempts made for a L2TP control packet.
l2tp tunnel retransmit timeout	Configures the amount of time that the router waits before resending an L2TP control packet.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.
vpdn-template	Creates a VPDN template and enters VPDN template configuration mode.

l2tp tunnel retransmit initial timeout

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

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

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

Syntax Description

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

Command Default

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

Command Modes

VPDN group configuration (config-vpdn)

VPDN template configuration (config-vpdn-temp)

Command History

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

Usage Guidelines

This command takes effect only when load balancing is enabled.

Control channel retransmissions follow an exponential backoff, starting at the minimum retransmit timeout length specified by the **min** *seconds* keyword and argument. After each packet that is not acknowledged,

the timeout exponentially increases until it reaches the value specified by the **max** *seconds* keyword and argument. For example, if the minimum timeout length is set to one second, the next retransmission attempt occurs two seconds later. The following attempt occurs four seconds later, and all additional attempts occur in eight second intervals.

Examples

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

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

Related Commands

Command	Description
l2tp tunnel busy timeout	Configures the amount of time that the router waits before attempting to recontact a router that was previously busy.
l2tp tunnel retransmit initial retries	Configures the number of times that the router attempts to send the initial L2TP control packet for tunnel establishment before considering a peer busy.
l2tp tunnel retransmit retries	Configures the number of retransmission attempts made for an L2TP control packet.
l2tp tunnel retransmit timeout	Configures the amount of time that the router waits before resending an L2TP control packet.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.
vpdn-template	Creates a VPDN template and enters VPDN template configuration mode.

l2tp tunnel retransmit retries

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

l2tp tunnel retransmit retries *number*

no l2tp tunnel retransmit retries *number*

Syntax Description

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

Command Default

The router resends control packets ten times.

Command Modes

VPDN group configuration (config-vpdn)

VPDN template configuration (config-vpdn-temp)

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

l2tp tunnel retransmit timeout

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

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

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

Syntax Description

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

Command Default

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

Command Modes

VPDN group configuration (config-vpdn)

VPDN template configuration (config-vpdn-temp)

Command History

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

Usage Guidelines

Control channel retransmissions follow an exponential backoff, starting at the minimum retransmit timeout length specified by the **min** *seconds* keyword and argument. After each packet that is not acknowledged, the timeout exponentially increases until it reaches the value specified by the **max** *seconds* keyword and argument. For example, if the minimum timeout length is set to 1 second, the next retransmission attempt

occurs 2 seconds later. The following attempt occurs 4 seconds later, and all additional attempts occur in 8-second intervals.

Cisco 10000 Series Router

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

Examples

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

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

Related Commands

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

l2tp tunnel timeout no-session

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

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

no l2tp tunnel timeout no-session

Syntax Description

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

Command Default

Empty tunnels are torn down after the default timeout.

Command Modes

VPDN group configuration (config-vpdn)

VPDN template configuration (config-vpdn-temp)

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

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

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

Related Commands

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

l2tp tunnel timeout setup

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

l2tp tunnel timeout setup *seconds*

no l2tp tunnel timeout setup *seconds*

Syntax Description

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

Command Default

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

Command Modes

VPDN group configuration (config-vpdn)

VPDN template configuration (config-vpdn-temp)

Command History

Release	Modification
12.1(1)	This command was introduced.

Usage Guidelines

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

Examples

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

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

Related Commands

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

l2tp tunnel zlb delay

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

l2tp tunnel zlb delay *seconds*

no l2tp tunnel zlb delay *seconds*

Syntax Description

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

Command Default

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

Command Modes

VPDN group configuration (config-vpdn)

VPDN template configuration (config-vpdn-temp)

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

l2tp tx-speed

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

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

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

Syntax Description

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

Command Default

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

Command Modes

VPDN group configuration (config-vpdn)

VPDN template configuration (config-vpdn-temp)

Command History

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

Usage Guidelines

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

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

Examples

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

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

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

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

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

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

Related Commands

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

lcp renegotiation

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

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

no lcp renegotiation

Syntax Description

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

Command Default

LCP renegotiation is disabled on the LNS.

Command Modes

VPDN group configuration (config-vpdn)

Command History

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

Usage Guidelines

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

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

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

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

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

Examples

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

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

Related Commands

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

loadsharing

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

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

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

Syntax Description

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

Command Default

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

Command Modes

VPDN group configuration (config-vpdn)

Command History

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

Usage Guidelines

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

Examples

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

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

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

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

Related Commands

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

local name

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

local name *host-name*

no local name

Syntax Description

host-name	Local hostname of the tunnel.

Command Default

No local hostname is configured.

Command Modes

VPDN group configuration (config-vpdn)

VPDN template configuration (config-vpdn-temp)

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

Related Commands

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