

# l2f ignore-mid-sequence

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  
VPDN template configuration

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 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, and 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
	<b>vpdn-group</b>	Creates a VPDN group and enters VPDN group configuration mode.
	<b>vpdn-template</b>	Creates a VPDN template and enters VPDN template configuration mode.

# l2f tunnel busy timeout

To configure the amount of time that the router will wait 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**

<b>Syntax Description</b>	<i>seconds</i>	Time, in seconds, to wait before checking for router availability. This value can range from 5 to 6000. The default value is 60.
---------------------------	----------------	--

<b>Command Default</b>	The router will wait 60 seconds before attempting to recontact a previously busy peer.
------------------------	--

<b>Command Modes</b>	VPDN group configuration VPDN template configuration
----------------------	---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(4)T	This command was introduced.
	12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco 1760, Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.

<b>Examples</b>	The following example configures the router to leave an L2F peer on the busy list for 90 seconds. This configuration applies only to tunnels associated with the virtual private dialup network (VPDN) group named group 1.
-----------------	---

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

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>l2f tunnel retransmit initial retries</b>	Configures the number of times that the router will attempt to send the initial control packet for tunnel establishment before considering an L2F peer busy.
	<b>l2f tunnel retransmit retries</b>	Configures the number of times the router will attempt to resend an L2F tunnel control packet before tearing the tunnel down.
	<b>l2f tunnel timeout setup</b>	Configures the amount of time that the router will wait for a confirmation message after sending out the initial L2F control packet before considering a peer busy.

<b>Command</b>	<b>Description</b>
<b>vpdn-group</b>	Creates a VPDN group and enters VPDN group configuration mode.
<b>vpdn-template</b>	Creates a VPDN template and enters VPDN template configuration mode.

## l2f tunnel retransmit initial retries

To configure the number of times that the router will attempt 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**

<b>Syntax Description</b>	<i>number</i>	The number of retries that will be attempted, ranging from 1 to 1000. The default value is 2.
---------------------------	---------------	---

**Command Default** The router will send the initial control packet twice.

**Command Modes** VPDN group configuration  
VPDN template configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(4)T	This command was introduced.
	12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco 1760, Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.

**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
	<b>l2f tunnel busy timeout</b>	Configures the amount of time that the router will wait before attempting to recontact an L2F peer that was previously busy.
	<b>l2f tunnel retransmit retries</b>	Configures the number of times the router will attempt to resend an L2F tunnel control packet before tearing the tunnel down.
	<b>l2f tunnel timeout setup</b>	Configures the amount of time that the router will wait for a confirmation message after sending out the initial L2F control packet before considering a peer busy.
	<b>vpdn-group</b>	Creates a VPDN group and enters VPDN group configuration mode.
	<b>vpdn-template</b>	Creates a VPDN template and enters VPDN template configuration mode.

## l2f tunnel retransmit retries

To configure the number of times the router will attempt 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**

<b>Syntax Description</b>	<i>number</i>	The number of retries that will be attempted, ranging from 5 to 1000. The default value is 6.
---------------------------	---------------	---

<b>Command Default</b>	The router will resend control packets six times.
------------------------	---

<b>Command Modes</b>	VPDN group configuration VPDN template configuration
----------------------	---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(4)T	This command was introduced.
	12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco 1760, Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.

<b>Usage Guidelines</b>	This command does not apply to the initial tunnel setup message or session control packets.
-------------------------	---

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

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

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>l2f tunnel busy timeout</b>	Configures the amount of time that the router will wait before attempting to recontact an L2F peer that was previously busy.
	<b>l2f tunnel retransmit initial retries</b>	Configures the number of times that the router will attempt to send the initial control packet for tunnel establishment before considering an L2F peer busy.

<b>Command</b>	<b>Description</b>
<b>l2f tunnel timeout setup</b>	Configures the amount of time that the router will wait for a confirmation message after sending out the initial L2F control packet before considering a peer busy.
<b>vpdn-group</b>	Creates a VPDN group and enters VPDN group configuration mode.
<b>vpdn-template</b>	Creates a VPDN template and enters VPDN template configuration mode.

# l2f tunnel timeout setup

To configure the amount of time that the router will wait for a confirmation message after sending out 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**

<b>Syntax Description</b>	<i>seconds</i>	Time, in seconds, that the router will wait for a return message. This value can range from 5 to 6000. The default value is 10.
---------------------------	----------------	---

<b>Command Default</b>	The router will wait 10 seconds for a confirmation message.
------------------------	---

<b>Command Modes</b>	VPDN group configuration VPDN template configuration
----------------------	---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(4)T	This command was introduced.
	12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco 1760, Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.

<b>Usage Guidelines</b>	If the router has not received a confirmation message from the peer device before the tunnel timeout setup timer expires, the peer will be placed on the busy list.
-------------------------	---

<b>Examples</b>	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 will apply only to tunnels associated with the virtual private dialup network (VPDN) group named group1.
-----------------	---

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

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>l2f tunnel busy timeout</b>	Configures the amount of time that the router will wait before attempting to recontact an L2F peer that was previously busy.
	<b>l2f tunnel retransmit initial retries</b>	Configures the number of times that the router will attempt to send the initial control packet for tunnel establishment before considering an L2F peer busy.

Command	Description
<b>l2f tunnel retransmit retries</b>	Configures the number of times the router will attempt to resend an L2F tunnel control packet before tearing the tunnel down.
<b>vpdn-group</b>	Creates a VPDN group and enters VPDN group configuration mode.
<b>vpdn-template</b>	Creates a VPDN template and enters VPDN template configuration mode.

# 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  
VPDN template configuraton

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
	<b>l2tp sequencing</b>	Enables sequencing for packets sent over an L2TP tunnel.
	<b>vpdn-group</b>	Creates a VPDN group and enters VPDN group configuration mode.
	<b>vpdn-template</b>	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**

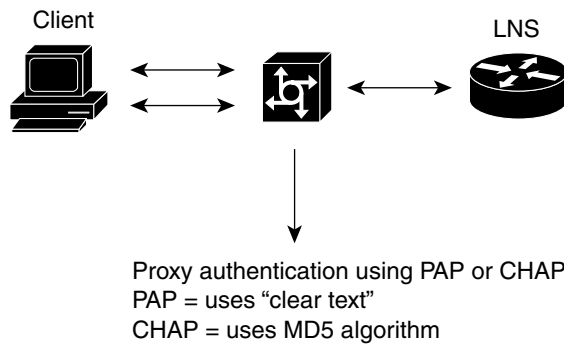
**Syntax Description** This command has no arguments or keywords.

**Command Default** L2TP AV pair hiding is disabled.

**Command Modes** VPDN group configuration  
VPDN template configuration

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 Layer 2 Tunneling Protocol 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 [Figure 1](#), 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 done 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, it is beneficial to use the **l2tp hidden** command where L2TP AV pair values are encrypted.

**Figure 1 LAC-LNS Proxy Authentication**

22105

**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
<b>vpdn-group</b>	Creates a VPDN group and enters VPDN group configuration mode.
<b>vpdn-template</b>	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  
VPDN template configuration

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 may be acceptable if the connection between the network access server (NAS) and the tunnel server is poor. Enabling IP UDP checksums will minimize 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
	<b>vpdn-group</b>	Creates a VPDN group and enters VPDN group configuration mode.
	<b>vpdn-template</b>	Creates a VPDN template and enters VPDN template configuration mode.

# I2tp security crypto-profile

To configure IP Security (IPSec) protection of Layer 2 Tunnel 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	
<i>profile-name</i>	The name of the crypto profile to be used for IPSec protection of tunneled PPP sessions. The <i>profile-name</i> argument must match the name of a profile configured using the <b>crypto map</b> command.
<b>keep-sa</b>	(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 <b>keep-sa</b> 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  
VPDN template configuration

Command History	Release	Modification
	12.2(4)T	This command was introduced.
	12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco 1760, Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.

**Usage Guidelines** A crypto profile must be configured using the **crypto map** (global IPSec) command before it can be associated with a VPDN group using the **l2tp security crypto-profile** command. Enabling this command for a VPDN group ensures that no L2TP packets will be processed unless they have IPSec protection.

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
<b>crypto map (global IPsec)</b>	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.
<b>vpdn-group</b>	Creates a VPDN group and enters VPDN group configuration mode.
<b>vpdn-template</b>	Creates a VPDN template and enters VPDN template configuration mode.

# I2tp sequencing

To enable sequencing for packets sent over a Layer 2 Tunnel 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  
VPDN template configuration

## 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 may 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 will not be 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 will include sequence numbers on data packets regardless of the **l2tp sequencing** command configuration.
- Enabling the **l2tp sequencing** command will cause 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 will include sequence numbers on data packets regardless of the **l2tp sequencing** command configuration.
- Enabling the **l2tp sequencing** command will cause 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 will send the Sequencing Required AV pair to the tunnel server, and sequencing will be 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
<b>l2tp drop out-of-order</b>	Instructs a NAS or tunnel server using L2TP to drop packets that are received out of order.
<b>vpdn-group</b>	Creates a VPDN group and enters VPDN group configuration mode.
<b>vpdn-template</b>	Creates a VPDN template and enters VPDN template configuration mode.

# 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  
VPDN template configuration

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
	<b>vpdn-group</b>	Creates a VPDN group and enters VPDN group configuration mode.
	<b>vpdn-template</b>	Creates a VPDN template and enters VPDN template configuration mode.

# I2tp tunnel bearer capabilities

To set the Layer 2 Tunnel Protocol (L2TP) bearer-capability value used by the Cisco router, use the **I2tp tunnel bearer capabilities** command in VPDN group or VPDN template configuration mode. To restore the default value, use the **no** form of this command.

**I2tp tunnel bearer capabilities** { **none** | **digital** | **analog** | **all** }

**no I2tp tunnel bearer capabilities**

## Syntax Description

<b>none</b>	Specifies that no access types are supported. This is the default value if the <b>accept-dialout</b> command is not configured..
<b>digital</b>	Specifies that digital access is supported.
<b>analog</b>	Specifies that analog access is supported.
<b>all</b>	Specifies that all access types are supported. This is the default value if the <b>accept-dialout</b> 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  
VPDN template configuration

## 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 may be required to override the default bearer-capability value by configuring the **I2tp 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
  I2tp tunnel bearer capabilities digital
```

**Related Commands**

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

# I2tp tunnel busy timeout

To configure the amount of time that the router will wait before attempting to recontact a Layer 2 Transport Protocol (L2TP) peer that was previously busy, use the **i2tp tunnel busy timeout** command in VPDN group or VPDN template configuration mode. To restore the default value, use the **no** form of this command.

**i2tp tunnel busy timeout** *seconds*

**no i2tp tunnel busy timeout**

<b>Syntax Description</b>	<i>seconds</i>	Time, in seconds, to wait before checking for router availability. This value can range from 5 to 6000. The default value is 60.
---------------------------	----------------	--

**Command Default** The router will wait 60 seconds before attempting to recontact a previously busy peer.

**Command Modes** VPDN group configuration  
VPDN template configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(4)T	This command was introduced.
	12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco 1760, Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.

**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
 i2tp tunnel busy timeout 90
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>i2tp tunnel retransmit initial retries</b>	Sets the number of times that the router will attempt to send out the initial control packet for tunnel establishment before considering a router busy.
	<b>i2tp tunnel retransmit initial timeout</b>	Sets the amount of time that the router will wait before resending an initial packet out to establish a tunnel.
	<b>vpdn-group</b>	Creates a VPDN group and enters VPDN group configuration mode.
	<b>vpdn-template</b>	Creates a VPDN template and enters VPDN template configuration mode.

# I2tp tunnel framing capabilities

To set the Layer 2 Tunnel 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

<b>none</b>	Specifies that no framing types are supported. This is the default value if the <b>accept-dialout</b> command is not configured.
<b>synchronous</b>	Specifies that synchronous framing is supported.
<b>asynchronous</b>	Specifies that asynchronous framing is supported.
<b>all</b>	Specifies that all framing types are supported. This is the default value if the <b>accept-dialout</b> 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  
VPDN template configuration

## 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 may 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:

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

Related Commands	Command	Description
	<b>accept-dialout</b>	Accepts requests to tunnel L2TP dial-out calls and creates an accept-dialout VPDN subgroup.
	<b>l2tp tunnel bearer capabilities</b>	Sets the bearer-capability value used by the Cisco router.
	<b>vpdn-group</b>	Creates a VPDN group and enters VPDN group configuration mode.
	<b>vpdn-template</b>	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 VPDN group or VPDN template configuration mode. To disable the sending of hello keepalive packets, use the **no** form of this command.

**l2tp tunnel hello** *seconds*

**no l2tp tunnel hello**

## Syntax Description

<i>seconds</i>	The interval, in seconds, that the network access server (NAS) and tunnel server wait before sending the next L2TP tunnel keepalive packet. Valid values range from 0 to 1000. The default value is 60.
----------------	---

## Command Default

Hello keepalive packets are sent every 60 seconds.

## Command Modes

VPDN group configuration  
VPDN template configuration

## 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.

## Examples

The following example sets the L2TP tunnel hello value to 90 seconds for tunnels associated with the virtual private dialup network (VPDN) group named group1:

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

## Related Commands

Command	Description
<b>vpdn-group</b>	Creates a VPDN group and enters VPDN group configuration mode.
<b>vpdn-template</b>	Creates a VPDN template and enters VPDN template configuration mode.

# l2tp tunnel password

To set the password that the router will use to authenticate Layer 2 Tunnel 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

<i>password</i>	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  
VPDN template configuration

## 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 will be used to authenticate tunnels associated with the virtual private dialup network (VPDN) group named group1:

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

**Related Commands**

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

# I2tp tunnel receive-window

To configure the number of packets allowed in the local receive window for a Layer 2 Tunnel Protocol (L2TP) control channel, use the **i2tp tunnel receive-window** command in VPDN group or VPDN template configuration mode. To restore the default value, use the **no** form of this command.

**i2tp tunnel receive-window** *packets*

**no i2tp tunnel receive-window** *packets*

<b>Syntax Description</b>	<i>packets</i>	Number of packets allowed in the receive window. Valid values range from 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  
VPDN template configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	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 **i2tp 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.

**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
 i2tp tunnel receive-window 500
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>vpdn-group</b>	Creates a VPDN group and enters VPDN group configuration mode.
	<b>vpdn-template</b>	Creates a VPDN template and enters VPDN template configuration mode.

## l2tp tunnel retransmit initial retries

To configure the number of times that the router will attempt to send out the initial Layer 2 Tunnel 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**

<b>Syntax Description</b>	<i>number</i>	Number of retransmission attempts. Valid values range from 1 to 1000. The default value is 2.
---------------------------	---------------	---

<b>Command Default</b>	The router will resend the initial L2TP control packet 2 times.
------------------------	---

<b>Command Modes</b>	VPDN group configuration VPDN template configuration
----------------------	---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(4)T	This command was introduced.
	12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco 1760, Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.

<b>Usage Guidelines</b>	Use the <b>l2tp tunnel retransmist initial retries</b> command to configure the number of times a device will attempt to resend the initial control packet used to establish an L2TP tunnel.
-------------------------	--

<b>Examples</b>	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
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>l2tp tunnel busy timeout</b>	Configures the amount of time that the router will wait before attempting to recontact a router that was previously busy.
	<b>l2tp tunnel retransmit initial timeout</b>	Configures the amount of time that the router will wait before resending an initial L2TP control packet out to establish a tunnel.
	<b>l2tp tunnel retransmit retries</b>	Configures the number of retransmission attempts made for a L2TP control packet.

<b>Command</b>	<b>Description</b>
<b>l2tp tunnel retransmit timeout</b>	Configures the amount of time that the router will wait before resending an L2TP control packet.
<b>vpdn-group</b>	Creates a VPDN group and enters VPDN group configuration mode.
<b>vpdn-template</b>	Creates a VPDN template and enters VPDN template configuration mode.

## l2tp tunnel retransmit initial timeout

To configure the amount of time that the router will wait before resending an initial Layer 2 Tunnel Protocol (L2TP) control packet out 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	max	seconds
	Specifies the minimum time that the router will wait before resending an initial packet.	Specifies the maximum time that the router will wait before resending an initial packet.	Timeout length, in seconds, the router will wait before resending an initial packet. Valid values range from 1 to 8. The default minimum value is 1. The default maximum value is 8.

**Command Default** The router will use the default timeout values specified in the “Syntax Description” section.

**Command Modes** VPDN group configuration  
VPDN template configuration

Command History	Release	Modification
	12.2(4)T	This command was introduced.
	12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco 1760, Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.

**Usage Guidelines** This command will take 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 combination. After each packet that is not acknowledged, the timeout exponentially increases until it reaches the value specified by the **max seconds** keyword and argument combination. 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.

**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 5 times before considering it busy. The timers are set so that the first attempt to recontact the peer will occur 2 seconds after the initial failure, and the final attempt will occur 7 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
<b>l2tp tunnel busy timeout</b>	Configures the amount of time that the router will wait before attempting to recontact a router that was previously busy.
<b>l2tp tunnel retransmit initial retries</b>	Configures the number of times that the router will attempt to send out the initial L2TP control packet for tunnel establishment before considering a peer busy.
<b>l2tp tunnel retransmit retries</b>	Configures the number of retransmission attempts made for an L2TP control packet.
<b>l2tp tunnel retransmit timeout</b>	Configures the amount of time that the router will wait before resending an L2TP control packet.
<b>vpdn-group</b>	Creates a VPDN group and enters VPDN group configuration mode.
<b>vpdn-template</b>	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 Tunnel 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

<i>number</i>	Number of retransmission attempts. Valid values range from 5 to 1000 retries. The default value is 10.
---------------	--

## Command Default

The router will resend control packets ten times.

## Command Modes

VPDN group configuration  
VPDN template configuration

## 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 retransmist retries** command to configure the number of times a device will attempt 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
<b>l2tp tunnel busy timeout</b>	Configures the amount of time that the router will wait before attempting to recontact a router that was previously busy.
<b>l2tp tunnel retransmit initial retries</b>	Configures the number of times that the router will attempt to send out the initial L2TP control packet for tunnel establishment before considering a peer busy.
<b>l2tp tunnel retransmit initial timeout</b>	Configures the amount of time that the router will wait before resending an initial L2TP control packet out to establish a tunnel.
<b>l2tp tunnel retransmit timeout</b>	Configures the amount of time that the router will wait before resending an L2TP control packet.

<b>Command</b>	<b>Description</b>
<b>l2tp tunnel timeout no-session</b>	Sets the duration a router waits after an L2TP tunnel becomes empty before tearing down the tunnel.
<b>vpdn-group</b>	Creates a VPDN group and enters VPDN group configuration mode.
<b>vpdn-template</b>	Creates a VPDN template and enters VPDN template configuration mode.

# l2tp tunnel retransmit timeout

To configure the amount of time that the router will wait before resending a Layer 2 Tunnel Protocol (L2TP) control packet, use the **l2tp tunnel retransmit timeout** command in VPDN group 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

<b>min</b>	Specifies the minimum time that the router will wait before resending a control packet.
<b>max</b>	Specifies the maximum time that the router will wait before resending a control packet.
<i>seconds</i>	Timeout length, in seconds, the router will wait before resending a control packet. Valid values range from 1 to 8. The default minimum value is 1. The default maximum value is 8.

## Command Default

The router will use the default timeout values specified in the “Syntax Description” section.

## Command Modes

VPDN group configuration  
VPDN template configuration

## 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

Control channel retransmissions follow an exponential backoff, starting at the minimum retransmit timeout length specified by the **min seconds** keyword and argument combination. After each packet that is not acknowledged, the timeout exponentially increases until it reaches the value specified by the **max seconds** keyword and argument combination. 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.

## 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
	<b>l2tp tunnel busy timeout</b>	Configures the amount of time that the router will wait before attempting to recontact a router that was previously busy.
	<b>l2tp tunnel retransmit initial retries</b>	Configures the number of times that the router will attempt to send out the initial L2TP control packet for tunnel establishment before considering a peer busy.
	<b>l2tp tunnel retransmit initial timeout</b>	Configures the amount of time that the router will wait before resending an initial L2TP control packet out to establish a tunnel.
	<b>l2tp tunnel retransmit retries</b>	Configures the number of retransmission attempts made for an L2TP control packet.
	<b>l2tp tunnel timeout no-session</b>	Sets the duration a router waits after an L2TP tunnel becomes empty before tearing down the tunnel.
	<b>vpdn-group</b>	Creates a VPDN group and enters VPDN group configuration mode.
	<b>vpdn-template</b>	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 Tunnel 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	<i>seconds</i>	<b>never</b>
	Time, in seconds, the router waits before tearing down an empty L2TP tunnel. Valid values range from 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.	Specifies that the router will never tear down an empty L2TP tunnel.

**Command Default** Empty tunnels will be torn down after the default timeout.

**Command Modes** VPDN group configuration  
VPDN template configuration

Command History	Release	Modification
	12.2(8)T	This command was introduced.
	12.2(11)T	Support was added for the <b>never</b> keyword.

**Usage Guidelines** Use the **l2tp tunnel timeout no-session** command to configure the amount of time a device will wait before tearing down an empty tunnel. It may 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
	<b>accept-dialin</b>	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.
	<b>accept-dialout</b>	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.
	<b>request-dialin</b>	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.
	<b>request-dialout</b>	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.
	<b>vpdn-group</b>	Creates a VPDN group and enters VPDN group configuration mode.
	<b>vpdn-template</b>	Creates a VPDN template and enters VPDN template configuration mode.

# I2tp tunnel timeout setup

To configure the amount of time that the router will wait for a confirmation message after sending out the initial Layer 2 Tunnel 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*

<b>Syntax Description</b>	<i>seconds</i>	Time, in seconds, the router will wait for a return message. Valid values range from 60 to 6000 seconds. The default value is 10 seconds.
---------------------------	----------------	---

<b>Command Default</b>	The router will wait 10 seconds for a confirmation message from the peer device before considering it busy.
------------------------	---

<b>Command Modes</b>	VPDN group configuration VPDN template configuration
----------------------	---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.1(1)	This command was introduced.

<b>Usage Guidelines</b>	If the router has not received a confirmation message from the peer device before the tunnel timeout setup timer expires, the peer will be placed on the busy list.
-------------------------	---

<b>Examples</b>	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 will apply only to tunnels associated with the virtual private dialup network (VPDN) group named group1.
-----------------	--

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

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>vpdn-group</b>	Creates a VPDN group and enters VPDN group configuration mode.
	<b>vpdn-template</b>	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*

<b>Syntax Description</b>	<i>seconds</i>	Maximum number of seconds the router will delay before acknowledging ZLB control messages. Valid values for the <i>seconds</i> argument range from 1 to 5. The default value is 3.
---------------------------	----------------	--

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

**Command Modes** VPDN group configuration  
VPDN template configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	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 may 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
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>vpdn-group</b>	Creates a VPDN group and enters VPDN group configuration mode.
	<b>vpdn-template</b>	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.
	<b>on-mismatch</b>	Renegotiate LCP at the LNS only in the event of an LCP mismatch between the LAC and LNS.

**Defaults** LCP renegotiation is disabled on the LNS.

**Command Modes** VPDN group configuration

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 will remove 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 may 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 will only occur if there is an LCP mismatch between the LNS and LAC.



**Note**

Older PC PPP clients may 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 pat
  lcp renegotiation on-mismatch
```

**Related Commands**

Command	Description
<b>accept-dialin</b>	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.
<b>force-local-chap</b>	Forces the LNS to reauthenticate the client.

# limit base-size

To define the base number of simultaneous connections that can be done in a single customer or virtual private dialup network (VPDN) profile, use the **limit base-size** command in customer profile configuration or VPDN profile configuration mode. To remove the limitation, use the **no** form of this command.

**limit base-size** {*base-number* | **all**}

**no limit base-size** {*base-number* | **all**}

## Syntax Description

<i>base-number</i>	Maximum number of simultaneous connections or sessions that can be used in a specified customer or VPDN profile, in the range from 0 to 1000.
<b>all</b>	Accept all calls (default). Use this keyword if you do not want to limit or apply overflow session counting to a customer or VPDN profile.

## Defaults

The base size is set to **all**.

## Command Modes

Customer profile configuration  
VPDN profile configuration

## Command History

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

## Usage Guidelines

Use the **limit base-size** command to define the base number of simultaneous connections in a single customer or VPDN profile. The session limit applies to all the physical resource groups and pools configured in a single customer profile. If you want to define the number of overflow calls granted to a customer profile by using the **limit overflow-size** command, do *not* use the **all** keyword in the **limit base-size** command; instead, specify a base number.

## Examples

The following example shows the total number of simultaneous connections limited to a base size of 48:

```
resource-pool profile customer customer1_isp
  limit base-size 48
```

## Related Commands

Command	Description
<b>limit overflow-size</b>	Defines the number of overflow calls granted to one customer or VPDN profile.
<b>resource-pool profile customer</b>	Creates a customer profile.

# limit overflow-size

To define the number of overflow calls granted to one customer or virtual private dialup network (VPDN) profile, use the **limit overflow-size** command in customer profile configuration or VPDN profile configuration mode. To remove the overflow configuration, use the **no** form of this command.

**limit overflow-size** {*overflow-calls* | **all**}

**no limit overflow-size** {*overflow-calls* | **all**}

## Syntax Description

<i>overflow-calls</i>	Number of overflow calls to grant, in the range from 0 to 1000. Default is 0.
<b>all</b>	Accept all overflow calls.

## Defaults

The overflow size is set to 0.

## Command Modes

Customer profile configuration  
VPDN profile configuration

## Command History

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

## Usage Guidelines

Use the **limit overflow-size** customer or VPDN profile configuration command to define the number of overflow calls granted to one customer or VPDN profile. The overflow is not applied if the **limit base-size** command is set using the **all** keyword.

## Examples

The following example shows 20 overflow calls granted to the customer profile called customer1\_isp:

```
resource-pool profile customer customer1_isp
  limit overflow-size 20
```

## Related Commands

Command	Description
<b>limit base-size</b>	Defines the base number of simultaneous connections that can be done in a single customer or VPDN profile.
<b>resource-pool profile customer</b>	Creates a customer profile.

# line-power

To configure an ISDN BRI port to supply line power to the terminal equipment (TE), use the **line-power** command in interface configuration mode. To disable the line power supply, use the **no** form of this command.

**line-power**

**no line-power**

## Syntax Description

This command has no arguments or keywords.

## Defaults

The BRI port does not supply line power.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.0(3)XG	This command was introduced on the Cisco MC3810 access concentrator.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.1(3)XI	This command was implemented on the Cisco 2600 and Cisco 3600 series.

## Usage Guidelines

This command is supported only if an installed BRI voice module (BVM) or BRI VIC is equipped to supply line power (phantom power).

This command is used only on a BRI port operating in NT mode. A BRI port operating in TE mode is automatically disabled as a source of line power, and the **line-power** command is rejected.

When you use the **line-power** command, the line power provision is activated on a BRI port if the port is equipped with the hardware to supply line power. When you enter the **no line-power** command, the line power provision is deactivated on a BRI port.



### Note

If the BRI port is operating in NT mode, the **line-power** command will be accepted, but will have no effect if a BVM is not equipped to supply line power.

## Examples

The following example configures a BRI port to supply power to an attached TE device (only if the BVM is equipped to supply line power):

```
interface bri 1
 line-power
```

# 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

<b>ip</b> <i>ip-address</i>	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.
<b>limit</b> <i>session-limit</i>	(Optional) Limits sessions per load share. The limit has a range from 0 to 32,767 sessions. By default, no limit is set.

## Defaults

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

## Command Modes

VPDN group configuration

## 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
<b>request-dialin</b>	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 will use 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

<i>host-name</i>	Local hostname of the tunnel.
------------------	-------------------------------

## Command Default

No local hostname is configured.

## Command Modes

VPDN group configuration  
VPDN template configuration

## 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 Tunnel 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
<b>l2tp tunnel password</b>	Sets the password the router uses to authenticate the tunnel.
<b>username</b>	Establishes a username-based authentication system.

■ local name

<b>Command</b>	<b>Description</b>
<b>vpdn-group</b>	Creates a VPDN group and enters VPDN group configuration mode.
<b>vpdn-template</b>	Creates a VPDN template and enters VPDN template configuration mode.

# logging event nfas-status

To enable the production of log messages when ISDN layer 2 changes occur on NFAS D-channels. (Primary or Backup D-channels up/down, and active/alternate D-channel changes), use the **logging event nfas-status** command in interface configuration mode. To disable notification, use the no form of this command.

**logging event nfas-status**

**no logging event nfas-status**

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** Disabled (does not produce reports).

---

**Command Modes** Interface configuration

---

Release	Modification
12.2(13)T	This command was introduced.

---

---

**Usage Guidelines** This configuration command should be entered on each ISDN serial interface.

This configuration command should be entered when the user wishes to see the NFAS D-channel status changes. Should “logging event link-status” not be configured, no indication may be provided when the NFAS D-channel status changes.

---

**Examples** The following example shows how to enable the production of log messages when ISDN layer 2 changes occur on NFAS D-channels using the logging event nfas-status command.

```
Router(config-if)# logging event nfas-status
```

# loopback (controller e1)

To loop an entire E1 line (including all channel groups defined on the controller) toward the line and back toward the router or access server, use the **loopback** command in controller configuration mode. To remove the loop, use the **no** form of this command.

**loopback**

**no loopback**

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** Loopback function is disabled.

---

**Command Modes** Controller configuration

---

Command History	Release	Modification
	11.1	This command was introduced.

---



---

**Usage Guidelines** This command is useful for testing the DCE channel service unit/data service unit (CSU/DSU) itself. To display interfaces currently in loopback operation, use the **show interfaces loopback EXEC** command.

---

**Examples** The following example configures the loopback test on the E1 line:

```
controller e1 0
 loopback
```

---

Related Commands	Command	Description
	<b>show interfaces loopback</b>	Displays information about the loopback interface.

---

# loopback local (controller)

To loop an entire T1 line (including all channel groups defined on the controller) toward the line and the router or access server, use the **loopback local** command in controller configuration mode. To remove the loop, use the **no** form of this command.

**loopback local**

**no loopback local**

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** Loopback function is disabled.

---

**Command Modes** Controller configuration

---

Release	Modification
11.1	This command was introduced.

---

---

**Usage Guidelines** This command is useful for testing the DCE channel service unit/data service unit (CSU/DSU) itself. To display interfaces currently in loopback operation, use the **show interfaces loopback EXEC** command.

---

**Examples** The following example configures the loopback test on the T1 line:

```
controller t1 0
 loopback local
```

---

Command	Description
<b>show interfaces loopback</b>	Displays information about the loopback interface.

---

# loopback local (interface)

To loop a channelized T1 or channelized E1 channel group, use the **loopback local** command in interface configuration mode. To remove the loop, use the **no** form of this command.

**loopback local**

**no loopback local**

**Syntax Description** This command has no arguments or keywords.

**Defaults** Loopback function is disabled.

**Command Modes** Interface configuration

Command History	Release	Modification
	11.1	This command was introduced.

**Usage Guidelines** This command is useful for looping a single channel group in a channelized environment without disrupting the other channel groups.

To display interfaces currently in loopback operation, use the **show interfaces loopback EXEC** command.

**Examples** The following example configures the loopback test on the T1 line:

```
interface serial 1/0:22
 loopback local
```

Related Commands	Command	Description
	<b>show interfaces loopback</b>	Displays information about the loopback interface.

# loopback remote (controller)

To loop packets from a MultiChannel Interface Processor (MIP) through the channel service unit/data service unit (CSU/DSU), over a dedicated T1 link, to the remote CSU at the single destination for this T1 link and back, use the **loopback remote** command in controller configuration mode. To remove the loop, use the **no** form of this command.

**loopback remote**

**no loopback remote**

**Syntax Description** This command has no arguments or keywords.

**Defaults** Command is disabled.

**Command Modes** Controller configuration

Command History	Release	Modification
	11.1	This command was introduced.

**Usage Guidelines** This command applies only when the device supports the remote function. It is used for testing the data communication channels.

For MIP cards, this controller configuration command applies if *only one* destination exists at the remote end of the cloud, the entire T1 line is dedicated to it, and the device at the remote end is a CSU (not a CSU/DSU). This is an uncommon case; MIPs are not usually used in this way.

To display interfaces currently in loopback operation, use the **show interfaces loopback EXEC** command.

**Examples** The following example configures a remote loopback test:

```
interface serial 0
 loopback remote
```

Related Commands	Command	Description
	<b>show interfaces loopback</b>	Displays information about the loopback interface.