Chapter 37

# Layer Two Tunnelling Protocol (L2TP)

# Introduction

This chapter describes the router's implementation of the Layer Two Tunnelling Protocol (L2TP), support for L2TP on the router and how to configure and operate the router as an L2TP server.

L2TP provides a mechanism for tunnelling the link layer of PPP (HDLC or asynchronous HDLC) over the Internet.

In a traditional dial-up service, a remote user makes a connection via a modem to a dial-up server at the target site, typically a central head office site. If the remote user and the central site are in different calling regions, the connection incurs toll call charges, rather than local calling charges. L2TP permits a dial-up server to be moved into the remote user's calling region and connected to the central site via an L2TP tunnel across the existing Internet infrastructure. The remote user can now make a local call to the dial-up server but the dial-up connection is terminated at the central site.

Traditional dial-up services only support users with registered IP addresses. L2TP provides virtual dial-up capabilities, enabling privately addressed IP and IPX dial-up via PPP to make use of the existing Internet infrastructure.

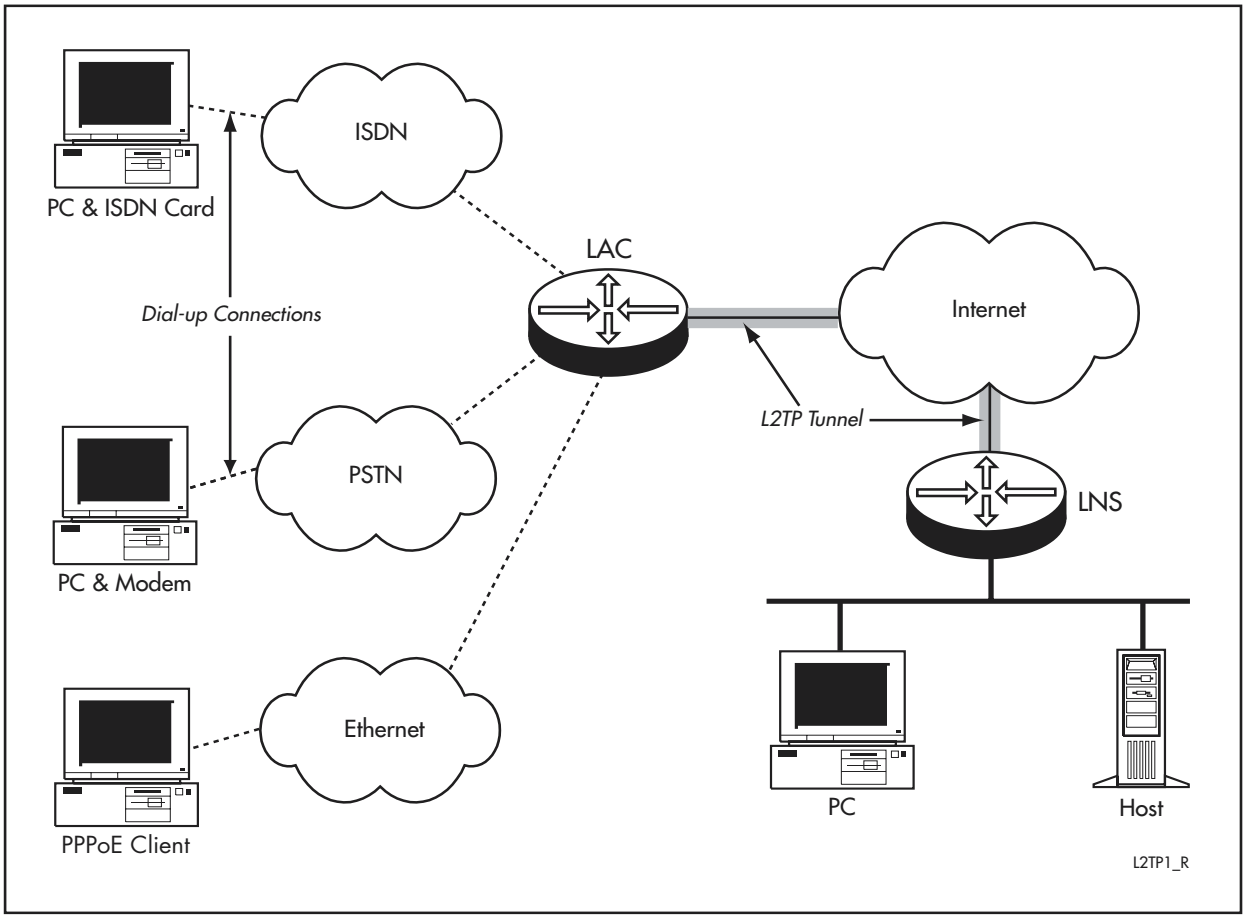
# Overview of L2TP

L2TP creates a tunnel across the Internet between an L2TP Access Concentrator (LAC) and an L2TP Network Server (LNS), enabling Point-to-Point Protocol (PPP) link layer frames to be encapsulated and carried across the Internet (Figure 37-1 on page 37-3). A remote user initiates a dial-up PPP connection to an *Internet Service Provider* (ISP) via a PSTN, ISDN or Ethernet service. The LAC accepts the connection and the PPP link is established. The ISP performs partial authentication in order to obtain the username of the dial-in user. The username can then be used to determine whether the user requires a virtual dial-up connection (using L2TP), or normal access to the Internet.

If a virtual dial-up connection is required, L2TP creates a tunnel (or uses an existing tunnel if one exists) to the endpoint, or LNS. An unused slot within the tunnel, or *Call Id* is allocated and the connection request is passed to the remote LNS, which may accept or reject the connection request. The connection request may include the information required to allow the LNS to authenticate the user and accept or decline the connection. For CHAP authentication, the connection request includes the challenge, username and raw responses. For PAP the connection request includes the username and plaintext password. The LNS may use the information to complete authentication, avoiding an additional cycle of authentication, or let PPP complete the authentication.

If the LNS accepts the connection, it creates a virtual PPP interface as if the dial-up connection was made directly to the LNS. Link layer frames can now pass over the tunnel. Frames received by the LAC are stripped of their CRC, link framing and transparency bytes, encapsulated in L2TP and forwarded over the appropriate tunnel. At the remote end of the tunnel, the LNS accepts the frames, strips off the L2TP encapsulation and processes the frames as normal incoming frames for the interface and protocol. For example, PPP packets are passed to PPP as if they had come directly from the HDLC link layer.

Figure 37-1: Model for implementing the Layer Two Tunnelling Protocol (L2TP)




The remote dial-in user is now effectively a dial-in PPP client of the LNS. Authorisation, protocol access and filtering can now be handled by the LNS using traditional methods. For example, the LNS may use a RADIUS server at the LNS site to authenticate the remote user.

# L2TP on the Router

The router implements L2TP as defined in RFC 2661, *Layer Two Tunnelling Protocol (L2TP)*.

A dial-in ACC call, ISDN call, or PPPoE session creates a dynamic PPP interface which starts Link Control Protocol (LCP) negotiation. When sufficient authentication information has been gathered by the LCP, a request is made to L2TP to determine (based on the user's login name), whether to create a L2TP tunnel to an L2TP LNS server, or create an Internet session directly as is normally the case. If L2TP determines it should create or use an existing tunnel to the remote LNS server, L2TP takes control of the lower layer interface and the current PPP session is terminated.

The router does not pass optional LCP configuration request information in L2TP incoming connection request messages.

To enable L2TP use the **enable l2tp** command on page 37-22. To disable it, use the **disable l2tp** command on page 37-21.

The router can be configured to act as an LAC, an LNS, or both by using the **enable l2tp server** command on page 37-24 and the **disable l2tp server** command on page 37-22.

To enable debugging on a per-call or per-tunnel basis, use the **enable l2tp debug** command on page 37-23. Disable debugging with the **disable l2tp debug** command on page 37-21.

In a typical scenario, L2TP supports only one-way dial-up connections. That is, a remote user dials into an ISP via the PSTN or via ISDN or starts a PPPoE session to the ISP. Once the connection has been made, data can be transferred in both directions. A less common scenario is a two-way dial-up connection, where the user can dial into the ISP and the ISP can dial into the user. Two-way dial-up connections are supported by PSTN and ISDN only.

When a remote user dials into a router enabled for L2TP, L2TP determines how to handle the call. An ACC call must be defined to answer the dial-up connection. See Chapter 28, Asynchronous Call Control for detailed information about defining an ACC call. Once the call has been answered by an ACC call, L2TP must decide how to handle the call. To create a mapping between a username or range of them and an action, use the **add l2tp user** command on page 37-16. To modify a mapping, use the **show l2tp user** command on page 37-44.

If a user connects via an ACC call with a username matching a map entry with an **action** of **ignore**, L2TP ignores the call and a normal Internet connection is made. Any other action causes L2TP to create an L2TP tunnel. The particular action specified determines how L2TP retrieves the information it needs to create the tunnel, such as the IP address of the remote L2TP server. To delete a username mapping, use the **delete l2tp user** command on page 37-20.

To display information about the currently defined mappings, use the **show l2tp user** command on page 37-44.

If two-way dial-up connections are required, an L2TP call must be defined on the LNS to enable the LNS to call back to the remote user. To create an L2TP call, use the **add l2tp call** command on page 37-13. To modify one, use the **set l2tp call** command on page 37-24.

The **type** parameter specifies the type of call the router at the remote end of the L2TP tunnel (acting as a LAC) uses to make the final connection to the remote user. The **remotecall** parameter specifies the name of this ACC, ISDN, or L2TP call, and must identify a call defined on the LAC.

When an LNS router makes an L2TP call to a remote user, the L2TP call connects the router to the remote L2TP server (the LAC) and passes the value of the **remotecall** parameter in the call setup message to the LAC. The LAC then makes a call to the remote user using the ACC, ISDN or L2TP call. When the remote user answers, a dial-up connection is established via the L2TP tunnel between the local LNS and the remote user.

When configuring an inter-router tunnel (**type=virtual**), the **remote** parameter should be used to identify an L2TP call defined on the remote router. Defining an L2TP call at both ends of an inter-router tunnel allows static PPP interfaces to be created at each end of the L2TP tunnel.

A statically defined L2TP call can be configured to call other LNSs that may not be configured to receive a specified remote L2TP call. To do this, set the **type** parameter to **virtual** and omit the **remote** parameter. On the remote router, a dynamic PPP interface is created to use the L2TP tunnel.

If a virtual L2TP call is required to be made in one direction only, set the IP parameter on the router at one end to 0.0.0.0, so that it can receive but not send this L2TP call.

To delete an L2TP call, use the **delete l2tp call** command on page 37-19.

To display information about the currently defined or active L2TP calls, use the **show l2tp call** command on page 37-33.

L2TP calls can be manually activated by using the **activate l2tp call** command on page 37-12. Deactivate calls with the **deactivate l2tp call** command on page 37-18.

To display the current state of L2TP, use the **show l2tp** command on page 37-29. Display active tunnels with the **show l2tp tunnel** command on page 37-36.

The PPP interfaces created at either end of an L2TP tunnel are typically dynamic PPP interfaces—they are created and destroyed dynamically in response to the activation or deactivation of ACC calls, ISDN calls, L2TP calls, or PPPoE sessions. PPP templates can be used to configure these dynamic interfaces.

When the ACC or ISDN call is activated and the LAC creates an L2TP tunnel to the remote L2TP peer, a dynamic PPP interface is created on the remote LT2P peer (the LNS), and the PPP template is used to configure this PPP interface.

PPP templates and other call attributes such as data packet sequence numbering and pre-Internet Draft 13 support, can also be associated with incoming L2TP calls on an LNS by using the **add l2tp ip** command on page 37-15.

When the LNS receives an L2TP call from an L2TP peer with a matching IP address, a dynamic PPP interface is created over the L2TP tunnel, and the PPP template is used to configure the PPP interface. The **number** parameter is used to determine how the LNS handles data packet sequence numbering for the call. L2TP Internet Drafts prior to Draft 13 are incompatible with Internet Drafts 13 and later. The **pre13** parameter allows compatibility with older implementations of L2TP.

To remove the association between an IP address and a PPP template, use the **delete l2tp ip** command on page 37-19.

To display the current associations between IP addresses and PPP templates, use the **show l2tp ip** command on page 37-35.

## Passwords in L2TP

A router that is acting as an L2TP LAC uses the password specified by the following commands:

- add l2tp call
- set l2tp call
- add l2tp user
- set l2tp user

A switch that is acting as an L2TP LNS uses the password specified by the **add l2tp password** command. If the IP address of the LAC exists in more than one password range on the LNS, then the password matching the smallest IP range is used. If there are IP ranges of equal size, then the range with the lowest base IP address is used.

To display L2TP passwords configured on the router, use the **show l2tp** command on page 37-29.

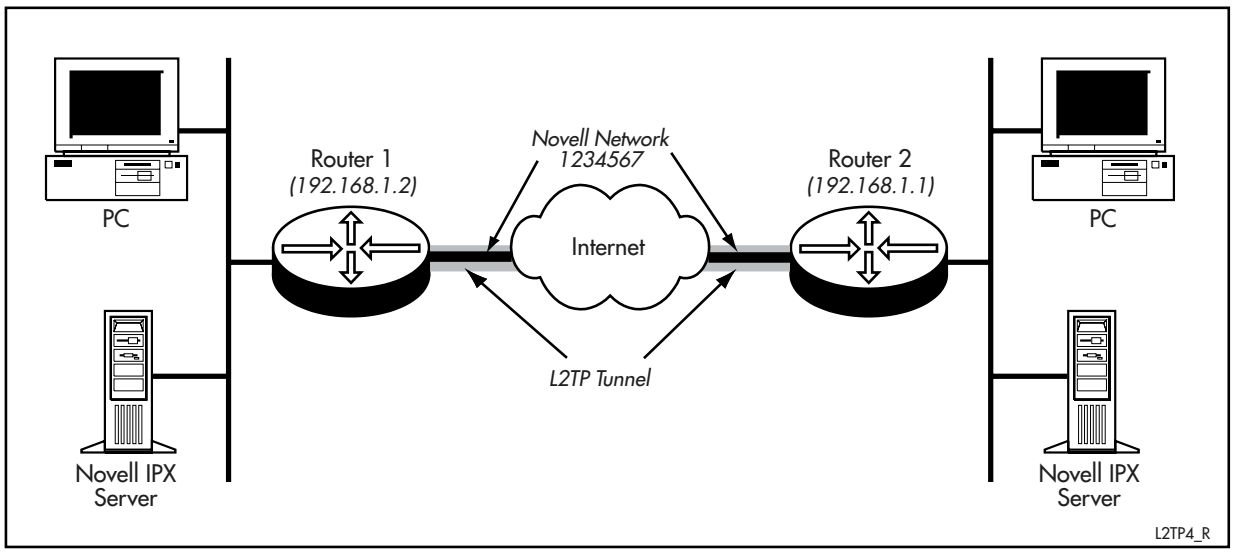
# Configuration Examples

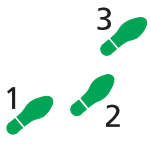
The following examples illustrate some ways that L2TP can be configured.

## Inter-Router Tunnels

The following example shows how to configure an L2TP tunnel between two routers. The configuration on each router is almost identical, except that calls from one router takes priority if both routers try to activate an L2TP call at the same time. This configuration allows the tunnelling of IPX traffic over the Internet (Figure 37-2 on page 37-6).

Figure 37-2: Configuration for inter-router L2TP tunnels




### To configure Router 1

1. **Enable the router as both a LAC and an LNS server.**

   Enable L2TP in both LAC and LNS server modes on the router:

   ```
   enable l2tp
   enable l2tp server=both
   ```

2. **Add the password for authenticating tunnel creation.**

   The Router 1 L2TP server expects the Router 2 L2TP server to use the password “verysecret” to authenticate the creation of new L2TP tunnels:

   ```
   add l2tp password=verysecret
   ```

**3. Create a static L2TP call to allow calls from Router 1 to Router 2.**

Create a static L2TP call with the static IP address 192.168.1.1 of Router 2. The password "verysecret" is used to authenticate the tunnel creation with the Router 2 L2TP server. Outgoing calls to Router 2 have precedence over incoming calls from Router 2:

```
add l2tp call=test remote=test type=virtual prec=out
   password=verysecret ip=192.168.1.1
```

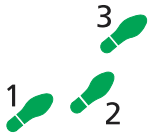
Create a PPP interface to use the L2TP call and enable IPX over the PPP interface:

```
create ppp=0 over=tnl-test idle=60

enable ipx

add ipx circ=1 int=ppp0 network=1234567 demand=on
```

IPX traffic destined for the IPX network 1234567 causes an L2TP tunnel to be created to Router 2.




### To configure Router 2

**1. Enable the router as both a LAC and an LNS server.**

Enable L2TP in both LAC and LNS server modes on the router:

```
enable l2tp

enable l2tp server=both
```

**2. Add the password for authenticating tunnel creation.**

The Router 2 L2TP server expects the Router 1 L2TP server to use the password "verysecret" to authenticate the creation of new L2TP tunnels:

```
add l2tp password=verysecret
```

**3. Create a static L2TP call to allow calls from Router 2 to Router 1.**

Create a static L2TP call with the static IP address 192.168.1.2 of Router 1. The password "verysecret" is used to authenticate the tunnel creation with the Router 1 L2TP server. Incoming calls from Router 1 have precedence over outgoing calls to Router 1:

```
add l2tp call=test remote=test type=virtual prec=in
   password=verysecret ip=192.168.1.2
```

Create a PPP interface to use the L2TP call and enable IPX over the PPP interface:

```
create ppp=0 over=tnl-test idle=60

enable ipx

add ipx circ=1 int=ppp0 network=1234567 demand=on
```

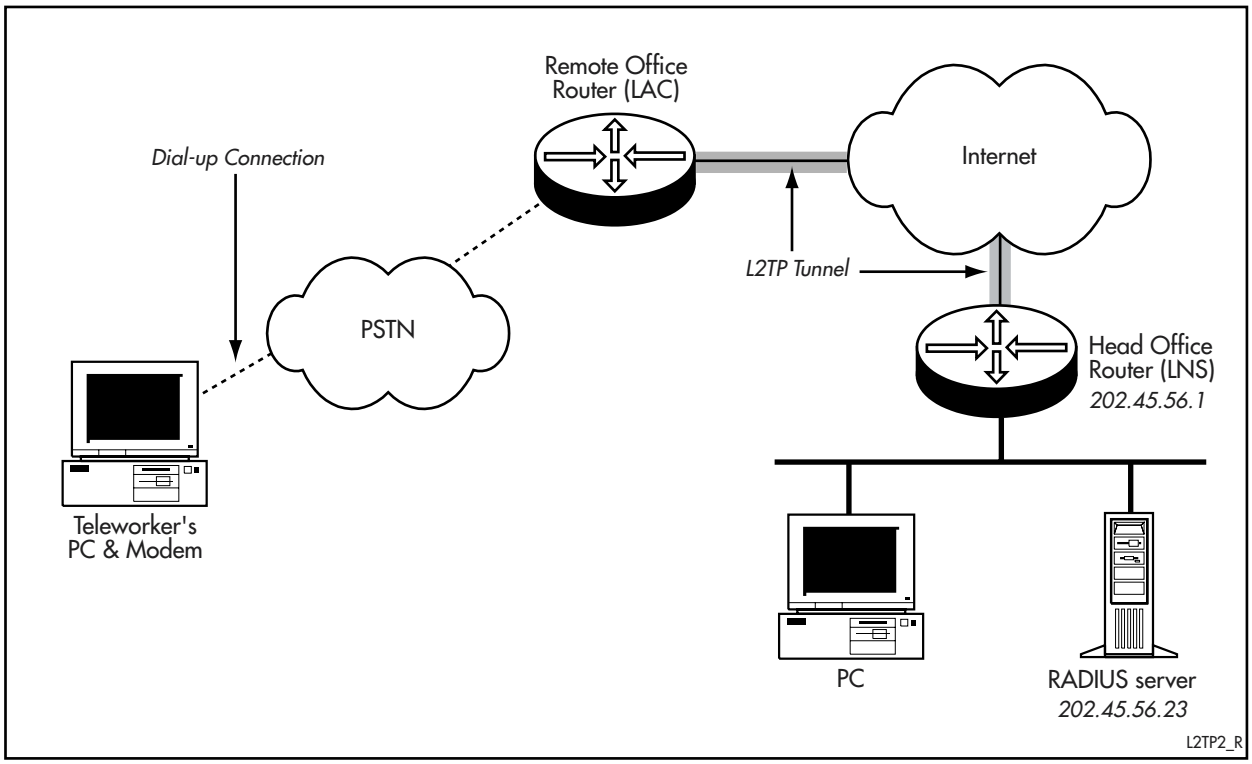
IPX traffic destined for the IPX network 1234567 causes an L2TP tunnel to be created to Router 2.

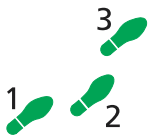
## Simple Dial-In System

This example explains show to configure a simple dial-in system. A company wants to allow teleworkers secure access to the company's head office site, but these workers are all in another telephone district. This would normally lead to expensive telephone bills. The solution is to locate a router in the teleworkers' telephone district to act as a clearing house, and then connect that router via a VPN to a router at the head office site. The router at the head office site acts as the termination point for the remote VPN and the access point for the remote teleworkers' traffic into the head office site. The benefit of this configuration is that the remote teleworker has access not only to the IP network, but also any IPX networks operating on the head office site.

The remote office router acts in L2TP terms as a LAC, and is connected to the Internet via a local ISP (*Internet Service Provider*). This router must have an asynchronous port and Asynchronous Call Control. All ACC calls, ISDN calls, and PPPoE sessions from teleworkers to the remote office router are automatically tunnelled through to the head office router. The head office router acts in L2TP terms as an LNS. Users are authenticated using RADIUS at the head office site (Figure 37-3 on page 37-8).

Figure 37-3: Configuration for a simple dial-in system using L2TP






### To configure the head office router

1. **Enable the router as an LNS.**

   Enable L2TP in LNS mode on the router:

   ```
   enable l2tp
   enable l2tp server=lns
   ```

2. **Configure the LNS to accept incoming L2TP tunnels.**

   Create a PPP Template to configure PPP sessions over the tunnel. Configure the router to accept L2TP tunnel creation requests from the remote office LAC, which is at the IP address 202.68.23.56.

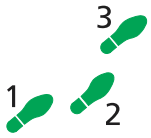
   ```
   create ppp template=1 auth=chap

   add l2tp ip=202.68.23.56 ppptemplate1=1
   ```

3. **Configure a RADIUS server to authenticate users.**

   The head office RADIUS server at IP address 202.45.56.23 authenticates the remote teleworkers:

   ```
   add radius server=202.45.56.23 secret="password"
   ```




### To configure the remote office router

1. **Create an ACC call to answer teleworkers dialling into the router.**

   Configure asynchronous port 2 for connection to an asynchronous modem. Create an ACC call to answer calls from the teleworkers' modems. Set the encapsulation to PPP. Create a PPP template, which is used to configure the PPP connection with CHAP authentication so that the teleworkers' username can be obtained:

   ```
   set asyn=2 flow=hardware speed=115200 cd=connect

   add acc call=teleworkers dir=ans encap=ppp asyn=2
      ppptemplate=1

   create ppp template=1 authen=chap
   ```

2. **Enable the router as an L2TP LAC.**

   Enable L2TP in LAC mode on the router:

   ```
   enable l2tp

   enable l2tp server=lac
   ```

3. **Configure the L2TP tunnel.**

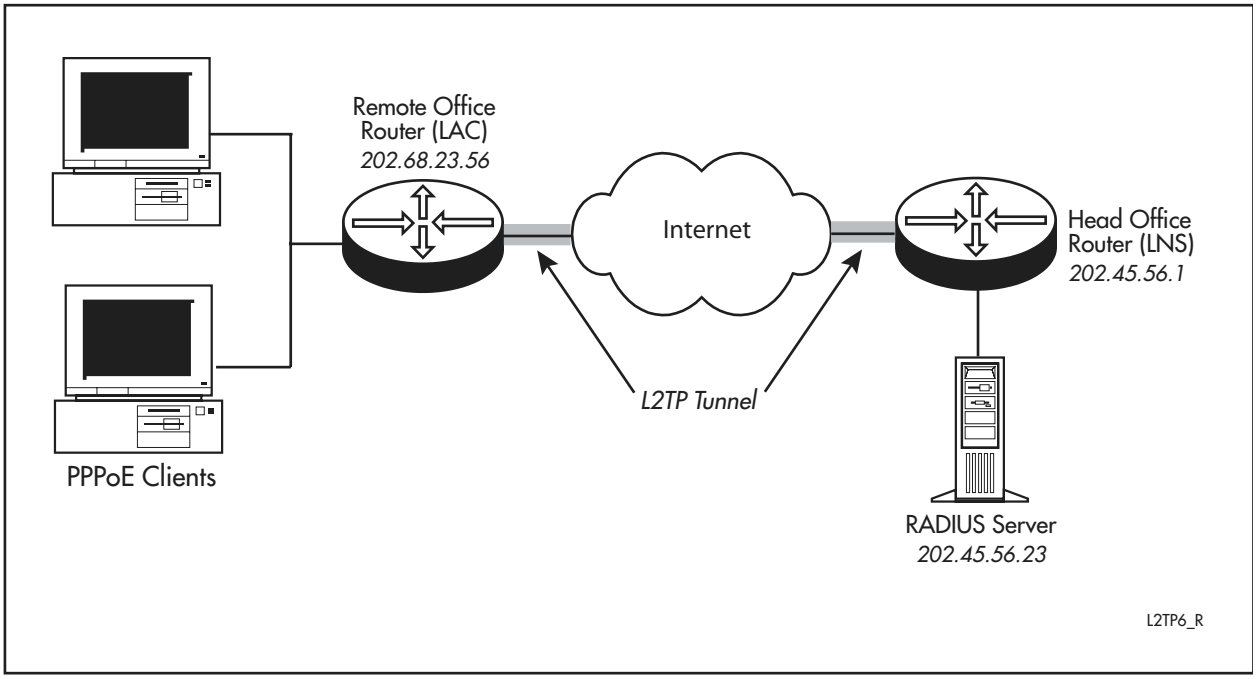
   Add a map entry to match the PPP usernames of the teleworkers, and activate an L2TP tunnel to the head office LNS with the IP address 202.45.56.1. Users are authenticated at the head office site using RADIUS:

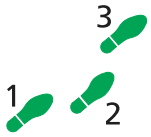
   ```
   add l2tp user=all action=database ip=202.45.56.1
   ```

# Configure L2TP to tunnel PPPoE sessions

This configuration shows how to configure L2TP to tunnel PPPoE sessions. In this example, a company wants to allow some users on the Ethernet network at the remote office access to the Ethernet network at the head office. One solution to this situation would be for each user to create a PPP session to the PPPoE Access Concentrator. The Access Concentrator then tunnels the PPP sessions to the head office site using L2TP. The remote office router acts in PPPoE terms as an Access Concentrator and in L2TP terms as a LAC. The head office router acts in L2TP terms as a LNS. Users are authenticated at the head office site using RADIUS (Figure 37-4 on page 37-10).

Figure 37-4: Configuration for L2TP to tunnel PPPoE sessions




## Configure the remote office router

**1. Define a PPP template used for PPPoE sessions.**

Define a PPP template that configures all PPP sessions between clients and the PPPoE Access Concentrator. A client's username is determined with Challenge Handshake Authentication Protocol (CHAP) authentication. This means L2TP can determine whether the user's PPP session should be tunnelled to the head office router. To create a PPP template called "1", and set its authentication to CHAP, use the command:

```
create ppp template=1

set ppp template=1 authentication=chap
```

**2. Configure the PPPoE Access Concentrator.**

Configure the remote office router to act as a PPPoE Access Concentrator. To make the "remote-office" router the Access Concentrator, using PPP template "1", and allowing only five users to access the head office site at one time, use the command:

```
add ppp acservice=remote-office template=1 maxsessions=5
   vlan=1

enable ppp accessconcentrator
```

3. **Enable the remote office router as a L2TP LAC server.**

   Configure the remote office router to act as a L2TP Access Concentrator (LAC):

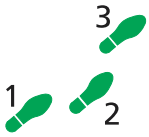
   ```
   enable l2tp

   enable l2tp server=lac
   ```

4. **Configure the L2TP tunnel.**

   To configure L2TP to tunnel all users to the LNS located at IP address 202.45.56.1, with the password "VERYSECRET", which is used by the router to authenticate tunnel creation with the head office LNS, use the command:

   ```
   add l2tp user=all action=database ip=202.45.56.1
      password=verysecret
   ```




## Configure the head office router

1. **Enable the router as an LNS.**

   To enable L2TP in LNS mode on the router, using the password "VERYSECRET", use the commands:

   ```
   enable l2tp

   enable l2tp server=lns

   add l2tp password=verysecret
   ```

2. **Configure the LNS to accept incoming L2TP tunnels.**

   To configure the router to accept L2TP tunnel creation requests from the remote office LAC, at IP address 202.68.23.56, using PPP template "1" to configure the PPP sessions over the tunnel, and enabling ECHO messages to determine link quality, use the commands:

   ```
   create ppp template=1 auth=chap echo=on

   add l2tp ip=202.68.23.56 ppptemplate=1
   ```

3. **Configure a RADIUS server to authenticate users.**

   To configure the head office RADIUS server at IP address 202.45.56.23 to authenticate the users from the remote office site use the command:

   ```
   add radius server=202.45.23.56 secret="password"
   ```

# Command Reference

This section describes the commands available on the router to configure and manage the Layer Two Tunnelling Protocol (L2TP).

L2TP requires the IP module to be enabled and configured correctly. Refer to Chapter 14, Internet Protocol (IP) for a detailed description of the commands required to enable and configure IP.

The shortest valid command is denoted by capital letters in the Syntax section. See "Conventions" on page xcv of Preface at the front of this manual for details of the conventions used to describe command syntax. See Appendix A, Messages for a complete list of messages and their meanings.

# activate l2tp call

**Syntax** `ACTivate L2TP CALL=`*`name`*

where *name* is an L2TP call name 1 to 15 characters long that is not case-sensitive. Valid characters are uppercase and lowercase letters, decimal digits (0–9) and the underscore character ("_").

**Description** This command activates a previously defined L2TP call. Using the predefined call information a call is made over L2TP to the remote L2TP server. The call must not already be active.

**Examples** To activate a predefined L2TP call named "home", use the command:

```
act l2tp call=home
```

**See Also** **add l2tp call**
**deactivate l2tp call**
**delete l2tp call**
**set l2tp call**
**show l2tp call**

# add l2tp call

**Syntax**

```
ADD L2TP CALL=name TYpe={ASYNc|ISDN|VIrtual} IP=ipadd
   REMotecall=name [DIAL=number] [NUMber={ON|OFF|STARTup}]
   [PASSword=password] [PRE13={ON|OFF}] [PRECedence={IN|
   OUT}] [SPeed=speed] [SUBAddress=subaddress]
```

where:

- *name* is an L2TP call name 1 to 15 characters long that is not case-sensitive. Valid characters are uppercase and lowercase letters, decimal digits (0–9), and the underscore character ("_").
- *ipadd* is an IP address in dotted decimal notation.
- *number* is a phone number 1 to 31 characters long. Valid characters are decimal digits (0–9).
- *password* is an authentication password 1 to 31 characters long that is case-sensitive. Valid characters are uppercase and lowercase letters, and decimal digits (0–9).
- *speed* is a decimal number from 300 to 4292967295.
- *subaddress* is a subaddress 1 to 31 characters long. Valid characters are uppercase and lowercase letters, and decimal digits (0–9).

**Description**

This command adds a call to a remote L2TP server. By associating a PPP interface with the call, PPP traffic to the remote L2TP server automatically activates a new L2TP tunnel, or use an existing L2TP tunnel, to the remote location.

The CALL parameter specifies the name of the L2TP call to add. An L2TP call with the same name must not already exist.

The TYPE parameter specifies the type of call the router at the remote end of the L2TP tunnel (acting as a LAC) uses to make the final connection to the remote user. If ASYNC is specified, an ACC call is used to connect to an analog modem. If ISDN is specified, an ISDN call is made. If VIRTUAL is specified an L2TP call is used to create a virtual link to another L2TP server.

The IP parameter specifies the IP address of the remote L2TP server, in dotted decimal notation. If the TYPE parameter is set to VIRTUAL, then the IP address can be set to 0.0.0.0. If IP is set to 0.0.0.0, then this end of the tunnel cannot initiate a virtual call to the remote end. It can, however, still respond to a virtual call from the remote end of the tunnel.

The REMOTECALL parameter specifies the name of an ACC call, an ISDN call, or another L2TP call on the remote L2TP server (the LAC). If the TYPE parameter is set to VIRTUAL and the REMOTECALL parameter is omitted, then the remote L2TP server creates a dynamic L2TP call in response to a call initiated from this router. The type of call must match the value specified for the TYPE parameter. For example, if TYPE is set to ASYNC, REMOTE must specify the name of an ACC call on the remote L2TP server.

The DIAL parameter specifies the number to be called to connect to the remote location, and must contain only the digits (including access codes and area codes) required to dial the remote L2TP server. The DIAL parameter is not supported by ACC and cannot be used if TYPE is set to ASYNC.

The NUMBER parameter specifies how L2TP handles the sequence numbering of L2TP data packets. If NUMBER is set to ON, data packets are always numbered. If NUMBER is set to OFF, only sequence numbering is used if the remote end requests sequencing. If NUMBER is set to STARTUP and the router is acting as an LNS, only sequence numbering is used during the initial PPP negotiation phase. After the initial PPP negotiation phase has concluded, sequence numbering of L2TP data packets ceases. L2TP data packet sequence numbering is used to ensure that packets arrive in the order in which they were sent from the remote L2TP server. This is required if encryption is active over the L2TP link. It is also useful in the initial PPP negotiation phase if the link between the L2TP servers uses multiple routes.

The PASSWORD parameter specifies a password to be used to authenticate the tunnel creation with the remote L2TP server.

The PRE13 parameter specifies compatibility with pre-Internet Draft 13 L2TP implementations.

The PRECEDENCE parameter specifies the direction of precedence for the L2TP call in the event of a call collision, and is only valid when TYPE is set to VIRTUAL. Call collision occurs when a call is activated at the same time as an incoming call selects the same call. If PRECEDENCE is set to IN, the incoming call is accepted and the outgoing call is cleared. If PRECEDENCE is set to OUT, the outgoing call proceeds and the incoming call is cleared. The default is IN.

The SPEED parameter specifies the maximum bandwidth of the connection, in bits per second. The default is 64000.

The SUBADDRESS parameter specifies an ISDN subaddress and is valid only when TYPE is set to ISDN.

**Examples** To add a call named “teleworker” over the Internet from a central office running an L2TP LNS server, via a branch office running an L2TP LAC server which has an ISDN call called “jimshome”, to a remote teleworker Jim, use the command:

```
add l2tp call=teleworker ty=isdn rem=jimshome ip=192.168.14.2
```

**See Also**
**activate l2tp call**
**deactivate l2tp call**
**delete l2tp call**
**set l2tp call**
**show l2tp call**

# add l2tp ip

**Syntax**

```
ADD L2TP IP=ipadd[-ipadd] PPPTemplate=ppp-template
   [NUMber={ON|OFF|STARTup}] [PRE13={ON|OFF}]
```

where:

- *ppp-template* is a number from 0 to 31.
- *ipadd* is an IP address in dotted decimal notation.

**Description**

This command associates a PPP template with incoming L2TP calls from an IP address or IP address range. When the LNS receives an L2TP call from a LAC with a matching IP address and a dynamic PPP interface is created, the associated PPP template is used to configure the PPP interface.This command is only valid on a router acting as an LNS.

The IP parameter specifies an IP address in dotted decimal notation, or a range of IP addresses. When the LNS receives an L2TP call from a LAC whose IP address matches the specified IP address (or falls within the specified range of IP addresses), the LNS creates a dynamic PPP interface over the L2TP tunnel using the specified PPP template.

The PPPTEMPLATE parameter specifies the PPP template to use when creating a dynamic PPP interface over the L2TP tunnel to the LAC. The specified template must exist. See "Templates" on page 9-18 of Chapter 9, Point-to-Point Protocol (PPP) for more information about creating PPP templates.

The NUMBER parameter specifies how L2TP handles the sequence numbering of L2TP data packets. If NUMBER is set to ON, data packets are always numbered. If NUMBER is set to OFF, only sequence numbering is used if the remote end requests sequencing. If NUMBER is set to STARTUP and the router is acting as an LNS, only sequence numbering is used during the initial PPP negotiation phase. After the initial PPP negotiation phase has concluded, sequence numbering of L2TP data packets ceases. L2TP data packet sequence numbering is used to ensure that packets arrive in the order in which they were sent from the remote L2TP server. This is required if encryption is active over the L2TP link. It is also useful in the initial PPP negotiation phase if the link between the L2TP servers uses multiple routes.

The PRE13 parameter specifies compatibility with pre-Internet Draft 13 L2TP implementations.

**Examples**

To configure an LNS to use PPP template 2 when creating dynamic PPP interfaces over L2TP tunnels to the L2TP LAC with the IP address 192.168.72.2, use the command:

```
add l2tp ip=192.168.74.2 pppt=2
```

To configure an LNS to use PPP template 1 when creating dynamic PPP interfaces over L2TP tunnels to L2TP LACs with IP addresses from 192.168.75.1 to 192.168.75.3, use the command:

```
add l2tp ip=192.168.75.1-192.168.75.3 pppt=1
```

**See Also**

**delete l2tp ip**
**show l2tp ip**

# add l2tp password

**Syntax** `ADD L2TP PASSword={`*`password`*`|NONE} [IP=`*`ipadd`*`[-`*`ipadd`*`]]`

where:

- *ipadd* is an IP address in dotted decimal notation.
- *password* is an authentication password 1 to 31 characters long that is case-sensitive. Valid characters are uppercase and lowercase letters, and decimal digits (0-9).

**Description** This command sets the L2TP password used on the LNS for LAC connections originating from a specific IP address range.

The PASSWORD parameter specifies the password, or NONE if no password is required. The default IP range is 0.0.0.0 - 255.255.255.255.

The IP parameter specifies the range of IP addresses to which this password applies. If the IP address of the LAC is associated with more than one password on the LNS, then the password matching the smallest IP range is used. If there are IP ranges of equal size, then the range with the lowest base IP address is used. If an identical IP range exists, then the password added with the **add l2tp call** command on page 37-13 overwrites the password added with the **set l2tp password** command on page 37-27.

**Examples** To set the password for clients from 192.168.0.0 - 192.168.255.255 to “secret”, use the command:

```
add l2tp pass=secret IP=192.168.0.0-192.168.255.255
```

**See Also** **delete l2tp password**
**set l2tp password**
**show l2tp**

# add l2tp user

**Syntax**
```
ADD L2TP USer={mapping|ALL|LOCAL|NONE|REMote}
   ACtion={DATABase|DNSLookup|IGNore|RADius} [IP=ipadd
   [POrt=port]] [NUMber={ON|OFF}] [PASSword=password]
   [PRE13={ON|OFF}] [PREFix=prefix] [TIMEOut=timeout]
```

where:

- *mapping* is a structured username 1 to 63 characters long. Valid characters are any printable character.
- *ipadd* is an IP address in dotted decimal notation.
- *port* is a UDP port number.
- *password* is a string 1 to 31 characters long. Valid characters are any printable character.
- *prefix* is a string 1 to 63 characters long. Valid characters are any printable character.
- *timeout* is a number from 1 to 300.

**Description** This command adds a mapping between a username provided for PPP authentication and the action L2TP takes on matching that username. When a dynamic PPP session starts, it passes PPP authentication details to L2TP. If L2TP is disabled PPP handles the authentication. If L2TP is enabled then each of the USER mappings is checked to determine whether L2TP should authenticate the PPP connection and the type of authentication to perform.

The USER parameter specifies the type of PPP username to match. If NONE is specified, the map entry matches PPP sessions for which no authentication is required. If LOCAL is specified, the map entry matches any PPP sessions using a username without any domain name information for authentication (such as "teleworker"). If REMOTE is specified, the map entry matches any PPP sessions using a username with domain name information for authentication (such as "john@maker.com"). If ALL is specified, the map entry matches any PPP sessions using any username. If a structured username (normally a domain name) is specified, the map entry matches any PPP sessions using matching usernames for authentication. For example, to map all users with the username types "xxx@company.com" the mapping should be set to "company.com".

The ACTION parameter specifies the action to take when a PPP username matches the map entry. If DATABASE is specified the IP address and port information in the matching map entry is used to create an L2TP tunnel to the remote server. If DNSLOOKUP is specified the username information is used to perform a DNS lookup to determine the IP address of the remote L2TP server. If the DNS lookup succeeds then an L2TP tunnel is created to the remote server. If IGNORE is specified, L2TP ignores the authentication query from the dynamic PPP session. The PPP session continues as a normal PPP link and an L2TP tunnel is not created. If RADIUS is specified the domain name portion of the username mapping information is used to perform a RADIUS lookup to determine the IP address of the remote L2TP server. If ACTION is set to DATABASE the IP parameter (and optionally the PORT parameter) must also be specified.

The IP parameter specifies the IP address, in dotted decimal notation, of the remote L2TP server to call. When a PPP username matches a map entry and the ACTION is set to DATABASE, the L2TP server creates an L2TP tunnel to the remote L2TP server specified by the IP and PORT parameters. If IP is specified, the ACTION parameter must be set to DATABASE.

The PORT parameter specifies the UDP port number to connect to on the remote L2TP server. When a PPP username matches a map entry and the ACTION is set to DATABASE, the L2TP server creates an L2TP tunnel to the remote L2TP server specified by the IP and PORT parameters. If PORT is specified, the ACTION parameter must be set to DATABASE and the IP parameter must also be specified.

The NUMBER parameter specifies how L2TP handles the sequence numbering of L2TP data packets. If NUMBER is set to ON, data packets are always numbered. If NUMBER is set to OFF, only sequence numbering is used if the remote end requests sequencing. L2TP data packet sequence numbering is used to ensure that packets arrive in the order in which they were sent from the remote L2TP server. This is required if encryption is active over the L2TP link. It is also useful in the initial PPP negotiation phase if the link between the L2TP servers uses multiple routes.

The PASSWORD parameter specifies the password to use to authenticate the L2TP tunnel creation to the specific remote L2TP server.

The PRE13 parameter specifies compatibility with pre-Internet Draft 13 L2TP implementations.

The PREFIX parameter specifies a string to prepend to the domain name portion of the username mapping string before performing the DNS lookup. For example, if the prefix string is set to “l2tp” and the mapping string is “john@maker.com”, then a DNS lookup is performed on the string “l2tp.maker.com”. The PREFIX parameter is only valid when ACTION is set to DNSLOOKUP.

The TIMEOUT parameter specifies the maximum round trip time, in seconds, for L2TP traffic.

**Examples** To add a record to map all users with usernames of the type “xxx@maker.com” to the remote L2TP server “l2tp.maker.com”, use the command:

```
add l2tp use=maker.com ac=dnsl pref=l2tp
```

**See Also** **delete l2tp user**
**set l2tp user**
**show l2tp user**

# deactivate l2tp call

**Syntax** `DEACTivate L2TP CALL={`*`name`*`|`*`callid`*`}`

where:

- *name* is an L2TP call name 1 to 15 characters long that is not case-sensitive. Valid characters are uppercase and lowercase letters, decimal digits (0–9), and the underscore character ("_").
- *callid* is the call identification number of a dynamic call from 1 to 65535.

**Description** This command deactivates the specified L2TP call. An L2TP call can be identified either by its name (for a predefined call), or by its dynamic call identification number. The call identification number can be determined from the output of the **show l2tp tunnel** command on page 37-36. The specified call must currently be active.

**Examples** To deactivate a L2TP call named “home”, use the command:

```
deact l2tp call=home
```

**See Also** **activate l2tp call**
**add l2tp call**
**delete l2tp call**
**set l2tp call**
**show l2tp call**

# delete l2tp call

**Syntax** `DELete L2TP CALL=`*`name`*

where *name* is an L2TP call name 1 to 15 characters long that is not case-sensitive. Valid characters are uppercase and lowercase letters, decimal digits (0–9), and the underscore character ("_").

**Description** This command deletes the specified predefined call to a remote L2TP server. The specified L2TP call must already exist.

**Examples** To delete a call called “teleworker”, use the command:

```
del l2tp call=teleworker
```

**See Also** **activate l2tp call**
**add l2tp call**
**deactivate l2tp call**
**set l2tp call**
**show l2tp call**

# delete l2tp ip

**Syntax** `DELete L2TP IP=`*`ipadd`*`[-`*`ipadd`*`]`

where:

- *ipadd* is an IP address in dotted decimal notation.

**Description** This command deletes the association between a PPP template and incoming L2TP calls from an IP address or IP address range. When the LNS receives an L2TP call from a LAC with a matching IP address and creates a dynamic PPP interface, the associated template is no longer used to configure the PPP interface. This command is only valid on a router acting as an LNS.

**Examples** To stop L2TP calls from the LAC with the IP address 192.168.72.2 creating dynamic PPP interfaces using PPP template 2, use the command:

```
del l2tp ip=192.168.74.2
```

**See Also** **add l2tp ip**
**show l2tp ip**

# delete l2tp password

**Syntax** `DELete L2TP PASSword [IP=`*`ipadd`*`{-`*`ipadd`*`]|ALL}]`

where:

- *ipadd* is an IP address in dotted decimal notation.
- *password* is an authentication password 1 to 31 characters long. Valid characters are letters (a-z, A-Z) and decimal digits (0-9). It is case sensitive.

**Description** This command removes the L2TP password used on an LNS for LAC connections originating from a specific IP address range. This command does not affect passwords set using the SET L2TP PASSWORD command.

The IP parameter specifies the range of IP addresses to remove a password from. The specified range must match an existing password range. If ALL is specified, then all passwords attached to ranges are removed.The default IP range is 0.0.0.0 - 255.255.255.255.

**Examples** To remove the existing password range 192.168.0.0 - 192.168.255.255, use the command:

```
del l2tp pass IP=192.168.0.0-192.168.255.255
```

**See Also** **add l2tp password**
**set l2tp password**
**show l2tp**

# delete l2tp user

**Syntax** `DELete L2TP USer={`*`mapping`*`|ALL|LOCAL|NONE|REMote}`

where *mapping* is a structured username 1 to 63 characters long. Valid characters are any printable character.

**Description** This command deletes a mapping between a username provided for PPP authentication and the action L2TP takes on matching that username.

**Examples** To delete a record used to map all users with usernames of the type “xxx@maker.com” to the remote L2TP server “l2tp.maker.com”, use the command:

```
del l2tp us=maker.com
```

**See Also** **add l2tp user**
**set l2tp user**
**show l2tp user**

# disable l2tp

**Syntax** `DISable L2TP`

**Description** This command disables L2TP tunnels so that they are not activated by the associated incoming ACC call, ISDN or L2TP call, or PPPoE sessions. L2TP is disabled by default.

**Examples** To disable L2TP, use the command:

```
dis l2tp
```

**See Also**
**disable l2tp debug**
**disable l2tp server**
**enable l2tp**
**enable l2tp debug**
**enable l2tp server**
**show l2tp**

# disable l2tp debug

**Syntax**
```
DISable L2TP DEBug={ALL|PKT|STAte} {CALL[=callid]|
   TUNnel[=tunnelId]}
```

where:

- *callid* is the call identification number of a dynamic call from 1 to 65535.
- *tunnelId* is the tunnel Id number of an L2TP tunnel from 1 to 65535.

**Description** This command disables debugging of the specified tunnel or call.

The DEBUG parameter specifies the debug options to disable. If ALL is specified, all debugging is disabled. If PKT is specified the display of packets passing through the specified tunnel or call is disabled. If STATE is specified the display of state transitions for the specified tunnel or call is disabled.

The CALL parameter specifies the L2TP call identification number for which debugging is to be disabled. If CALL is specified without a value, debugging is disabled for all currently active calls and all calls created from that time, until call debugging is enabled.

The TUNNEL parameter specifies the tunnel for which debugging is to be disabled. If TUNNEL is specified without a value, debugging is disabled for all currently active tunnels and all tunnels created from that time, until tunnel debugging is enabled.

**Examples** To disable all debugging of call 21, use the command:

```
dis l2tp deb=all call=21
```

**See Also**
disable l2tp
disable l2tp server
enable l2tp
enable l2tp debug
enable l2tp server
show l2tp

# disable l2tp server

**Syntax**
```
DISable L2TP SERVER={LNS|LAC|BOTH}
```

**Description**
This command selectively disables the server modes of the L2TP process.

The SERVER parameter specifies the L2TP server mode to disable. If LNS is specified, the LNS server mode is disabled. In LNS mode the router acts as a termination point for L2TP tunnels and calls. If LAC is specified, the LAC server mode is disabled. In LAC mode the router intercepts ACC calls, ISDN calls, or PPPoE sessions and redirects them over L2TP tunnels to remote LNS servers. If BOTH is specified, both the LNS and LAC server modes are disabled. By default, both LNS and LAC server modes are disabled.

**Examples**
To disable L2TP LAC server mode, use the command:

```
dis l2tp server=lac
```

**See Also**
disable l2tp
disable l2tp debug
enable l2tp
enable l2tp debug
enable l2tp server
show l2tp

# enable l2tp

**Syntax**
```
ENAble L2TP
```

**Description**
This command enables incoming ACC calls, ISDN calls, L2TP calls or PPPoE so that sessions activate the associated L2TP call. L2TP is enabled by default.

**Examples**
To enable the L2TP module, use the command:

```
ena l2tp
```

**See Also**
disable l2tp
disable l2tp debug
disable l2tp server
enable l2tp debug
enable l2tp server
show l2tp

# enable l2tp debug

**Syntax**

```
ENAble L2TP DEBug={ALL|PKT|STAte} {CALL[=callid]|
   TUNnel[=tunnelId]}
```

where:

- *callid* is the call identification number of a dynamic call from 1 to 65535.
- *tunnelId* is the tunnel Id number of an L2TP tunnel from 1 to 65535.

**Description**

This command enables debugging of the specified tunnel or call.

The DEBUG parameter specifies the debug options to enable. If ALL is specified, all debugging is enabled. If PKT is specified the display of packets passing through the specified tunnel or call is enabled. If STATE is specified the display of state transitions for the specified tunnel or call is enabled.

The CALL parameter specifies the L2TP call identification number for which debugging is to be enabled. If CALL is specified without a value, debugging is enabled for all currently active calls and all calls created from that time, until call debugging is disabled.

The TUNNEL parameter specifies the tunnel for which debugging is to be enabled. If TUNNEL is specified without a value, debugging is enabled for all currently active tunnels and all tunnels created from that time, until tunnel debugging is disabled.

**Examples**

To enable packet debugging of call 34, use the command:

```
dis l2tp deb=pkt call=34
```

**See Also**

**disable l2tp**
**disable l2tp debug**
**disable l2tp server**
**enable l2tp**
**enable l2tp server**
**show l2tp**

# enable l2tp server

**Syntax** `ENAble L2TP SERVER={BOTH|LAC|LNS}`

**Description** This command selectively enables the server modes of the L2TP process.

The SERVER parameter specifies the L2TP server mode to enable. If LNS is specified, the LNS server mode is enabled. In LNS mode the router acts as a termination point for L2TP tunnels and calls. If LAC is specified, the LAC server mode is enabled. In LAC mode the router intercepts ACC calls, ISDN calls, or PPPoE sessions and redirects them over L2TP tunnels to remote LNS servers. If BOTH is specified, both the LNS and LAC server modes are enabled. By default, both LNS and LAC server modes are disabled.

**Examples** To enable a router to act as an L2TP LAC, use the command:

```
ena l2tp server=lac
```

**See Also** **disable l2tp**
**disable l2tp debug**
**disable l2tp server**
**enable l2tp**
**enable l2tp debug**
**show l2tp**

# set l2tp call

**Syntax**
```
SET L2TP CALL=name [TYpe={ASYNc|ISDN|VIrtual}] [IP=ipadd]
   [REMotecall=name] [DIAL=number] [NUMber={ON|OFF|
   STARTup}] [PASSword=password] [PRE13={ON|OFF}]
   [PRECedence={IN|OUT}] [SPeed=speed]
   [SUBAddress=subaddress]
```

where:

- *name* is an L2TP call name 1 to 15 characters long that is not case-sensitive. Valid characters are uppercase and lowercase letters, decimal digits (0–9), and the underscore character ("_").
- *ipadd* is an IP address in dotted decimal notation.
- *number* is a phone number 1 to 31 characters long. Valid characters are decimal digits (0–9).
- *password* is an authentication password 1 to 31 characters long that is case-sensitive. Valid characters are uppercase and lowercase letters, and decimal digits (0–9).
- *speed* is a decimal number from 300 to 4292967295.
- *subaddress* is a subaddress 1 to 31 characters long. Valid characters are uppercase and lowercase letters, and decimal digits (0–9).

**Description**

This command changes the attributes of a call to a remote L2TP server. By associating a PPP interface with the call, PPP traffic to the remote L2TP server automatically activates a new L2TP tunnel, or use an existing L2TP tunnel, to the remote location.

The CALL parameter specifies the name of the L2TP call to add. An L2TP call with the same name must not already exist.

The DIAL parameter specifies the number to be called to connect to the remote location, and must contain only the digits (including access codes and area codes) required to dial the remote L2TP server. The DIAL parameter is not supported by ACC and cannot be used if TYPE is set to ASYNC.

The IP parameter specifies the IP address of the remote L2TP server, in dotted decimal notation. If the TYPE parameter is set to VIRTUAL, then the IP address can be set to 0.0.0.0. If IP is set to 0.0.0.0, then this end of the tunnel cannot initiate a virtual call to the remote end. It can, however, still respond to a virtual call from the remote end of the tunnel.

The NUMBER parameter specifies how L2TP handles the sequence numbering of L2TP data packets. If NUMBER is set to ON, data packets are always numbered. If NUMBER is set to OFF, only sequence numbering is used if the remote end requests sequencing. If NUMBER is set to STARTUP and the router is acting as an LNS, only sequence numbering is used during the initial PPP negotiation phase. After the initial PPP negotiation phase has concluded, sequence numbering of L2TP data packets ceases. L2TP data packet sequence numbering is used to ensure that packets arrive in the order in which they were sent from the remote L2TP server. This is required if encryption is active over the L2TP link. It is also useful in the initial PPP negotiation phase if the link between the L2TP servers uses multiple routes.

The PASSWORD parameter specifies a password to be used to authenticate the tunnel creation with the remote L2TP server.

The PRE13 parameter specifies compatibility with pre-Internet Draft 13 L2TP implementations.

The PRECEDENCE parameter specifies the direction of precedence for the L2TP call in the event of a call collision, and is only valid when TYPE is set to VIRTUAL. Call collision occurs when a call is activated at the same time as an incoming call selects the same call. If PRECEDENCE is set to IN, the incoming call is accepted and the outgoing call is cleared. If PRECEDENCE is set to OUT, the outgoing call proceeds and the incoming call is cleared. The default is IN.

The REMOTECALL parameter specifies the name of either an ACC call, an ISDN call or another L2TP call on the remote L2TP server (the LAC). If the TYPE parameter is set to VIRTUAL and the REMOTECALL parameter is omitted, then the remote L2TP server creates a dynamic L2TP call in response to a call initiated from this router. (If the REMOTECALL parameter was previously set to a name, this name can be replaced, but not removed, by using the **set l2tp call** command on page 37-24. Use the **add l2tp call** command on page 37-13 to create a new call with the remote parameter omitted.) The type of call must match the value specified for the TYPE parameter. For example, if TYPE is set to ASYNC, REMOTECALL must specify the name of an ACC call on the remote L2TP server.

The SPEED parameter specifies the maximum bandwidth of the connection, in bits per second. The default is 64000.

The SUBADDRESS parameter specifies an ISDN subaddress and is valid only when TYPE is set to ISDN.

The TYPE parameter specifies the type of call the router at the remote end of the L2TP tunnel (acting as a LAC) uses to make the final connection to the remote user. If ASYNC is specified, an ACC call is used to connect to an analog modem. If ISDN is specified, an ISDN call is made. If VIRTUAL is specified an L2TP call is used to create a virtual link to another L2TP server.

**Examples** To change the call called "teleworker" over the Internet from a central office, via a branch office which has an ISDN call called johnshome, to a remote teleworker John, use the command:

```
set l2tp call=teleworker ty=ISDN suba=johnshome
```

**See Also**
**activate l2tp call**
**add l2tp call**
**deactivate l2tp call**
**delete l2tp call**
**show l2tp call**

# set l2tp checksum

**Syntax**

```
SET L2TP CHECKSum={ON|OFF}
```

**Description** This command enables or disables the calculation of checksums on UDP datagrams containing L2TP payload packets, for all tunnels and L2TP calls. Checksums should be disabled on payload packets only if the underlying network automatically corrects transmission errors. Checksums are always calculated for UDP datagrams containing L2TP control packets.

**Examples** To disable the calculation of checksums on UDP datagrams containing L2TP payload packets, use the command:

```
set l2tp checks=off
```

**See Also** **show l2tp**

# set l2tp filter

**Syntax**

```
SET L2TP FILter={filter-number|NONE}
```

where *filter-number* is the number of a predefined IP filter from 0 to 299

**Description** This command provides a mechanism to select the remote L2TP servers with which the router can communicate and form tunnels.

The FILTER parameter specifies an existing IP filter, or "NONE". If NONE is specified, filtering is disabled and there are no restrictions on the remote L2TP servers with which the router can communicate. If FILTER is set to a number it

must be the number of an existing IP filter which matches some combination of source address, destination address, protocol and/or port number. The router is only able to communicate with remote L2TP servers that are included by the IP filter. IP filters are created using the **add ip filter** command on page 14-68 of Chapter 14, Internet Protocol (IP).

**Examples** To use IP filter 2 to select the remote L2TP servers to communicate with, use the command:

```
set l2tp fil=2
```

**See Also** **show l2tp**

# set l2tp password

**Syntax**

```
SET L2TP PASSword={password|NONE}
```

where *password* is an authentication password 1 to 31 characters long that is case-sensitive. Valid characters are uppercase and lowercase letters, and decimal digits (0–9).

**Description** This command has been superseded by the **add l2tp password** and **delete l2tp password** commands. The **add l2tp password** command allows more than one password to be set on the L2TP LNS. The **create config** command converts **set l2tp password** commands to **add l2tp password** commands.

This command sets a global password to be used on an LNS when authenticating tunnel creation with all other L2TP servers. The PASSWORD parameter specifies the password, or NONE to delete the global password.

**Examples** To set the global password to "secret", use the command:

```
set l2tp pass=secret
```

**See Also** **show l2tp**

# set l2tp user

**Syntax**

```
SET L2TP USer={mapping|ALL|LOCAL|NONE|REMote}
   [ACtion={DATABase|DNSLookup|IGNore|RADius}] [IP=ipadd
   [POrt=port]] [NUMber={ON|OFF}] [PASSword=password]
   [PRE13={ON|OFF}] [PREFix=prefix] [TIMEOut=timeout]
```

where:

- *mapping* is a structured username 1 to 63 characters long. Valid characters are any printable character.
- *ipadd* is an IP address in dotted decimal notation.
- *port* is a UDP port number.

- *password* is a string 1 to 31 characters long. Valid characters are any printable character.
- *prefix* is a string 1 to 63 characters long. Valid characters are any printable character.
- *timeout* is a number from 1 to 300.

**Description** This command changes the attributes of a mapping between a username provided for PPP authentication and the action L2TP takes on matching that username. When a dynamic PPP session starts it passes PPP authentication details to L2TP. If L2TP is disabled, PPP handles the authentication. If L2TP is enabled, then each of the USER mappings is checked to determine whether L2TP should authenticate the PPP connection and the type of authentication to perform.

The USER parameter specifies the type of PPP username to match. If NONE is specified, the map entry matches PPP sessions for which no authentication is required. If LOCAL is specified, the map entry matches any PPP sessions using a username without any domain name information for authentication (e.g. “teleworker”). If REMOTE is specified, the map entry matches any PPP sessions using a username with domain name information for authentication (for example “longjohn@maker.com“). If ALL is specified, the map entry matches any PPP sessions using any username. If a structured username (normally a domain name) is specified, the map entry matches any PPP sessions using matching usernames for authentication. For example, to map all users with the username types “xxx@company.com”, the mapping should be set to “company.com”.

The ACTION parameter specifies the action to take when a PPP username matches the map entry. If DATABASE is specified, the IP address and port information in the matching map entry is used to create an L2TP tunnel to the remote server. If DNSLOOKUP is specified, the username information is used to perform a DNS lookup to determine the IP address of the remote L2TP server. If the DNS lookup succeeds, then an L2TP tunnel is created to the remote server. If IGNORE is specified, L2TP ignores the authentication query from the dynamic PPP session. The PPP session continues as a normal PPP link and an L2TP tunnel is not created. If RADIUS is specified, the domain name portion of the username mapping information is used to perform a RADIUS lookup to determine the IP address of the remote L2TP server. If ACTION is set to DATABASE, the IP parameter (and optionally the PORT parameter) must also be specified.

The IP parameter specifies in dotted decimal notation the IP address of the remote L2TP server to call. When a PPP username matches a map entry and the ACTION is set to DATABASE, the L2TP server creates an L2TP tunnel to the remote L2TP server specified by the IP and PORT parameters. If IP is specified, the ACTION parameter must be set to DATABASE.

The PORT parameter specifies the UDP port number to connect to on the remote L2TP server. When a PPP username matches a map entry and the ACTION is set to DATABASE, the L2TP server creates an L2TP tunnel to the remote L2TP server specified by the IP and PORT parameters. If PORT is specified, the ACTION parameter must be set to DATABASE and the IP parameter must also be specified.

The NUMBER parameter specifies how L2TP handles the sequence numbering of L2TP data packets. If NUMBER is set to ON, data packets are always numbered. If NUMBER is set to OFF, only sequence numbering is used if the remote end requests sequencing. L2TP data packet sequence numbering is

used to ensure that packets arrive in the order in which they were sent from the remote L2TP server. This is required if encryption is active over the L2TP link. It is also useful in the initial PPP negotiation phase if the link between the L2TP servers uses multiple routes.

The PASSWORD parameter specifies the password to use to authenticate the L2TP tunnel creation to the specific remote L2TP server.

The PRE13 parameter specifies compatibility with pre-Internet Draft 13 L2TP implementations.

The PREFIX parameter specifies a string to prepend to the domain name portion of the username mapping string before performing the DNS lookup. For example, if the prefix string is set to "l2tp" and the mapping string is "john@maker.com", then a DNS lookup is performed on the string "l2tp.maker.com". The PREFIX parameter is only valid when ACTION is set to DNSLOOKUP.

The TIMEOUT parameter specifies the maximum round trip time, in seconds, for L2TP traffic.

**Examples** To modify a record to map all users with usernames of the type "xxx@maker.com" to the remote LNS server "lns.maker.com", use the command:

```
set l2tp us=maker.com pref=lns
```

**See Also** **add l2tp password**
**delete l2tp user**
**show l2tp user**

# show l2tp

**Syntax** `SHow L2TP [COUnter]`

**Description** This command displays the global configuration and status of L2TP (Figure 37-5 on page 37-30, Table 37-1 on page 37-30).

The COUNTER parameter displays additional information about general counters for L2TP (Figure 37-6 on page 37-31, Table 37-2 on page 37-32).

Figure 37-5: Example output from the **show l2tp** command

```
L2TP Server

  State ............................ enabled
  Server ........................... both
  Passwords
  10.0.0.1 ........................  secret
  10.0.0.0 - 10.0.0.254 ...........  rose
  10.0.0.1 - 10.0.0.255 ...........  daphne
  0.0.0.0 - 255.255.255.255 .......  baserange
  Filter ........................... not set
  Default Call Receive Window ...... 16
  Checksum Payload Packets ......... on
  Failed Authentications ........... 0
  In Messages ...................... 3107
  Out Messages ..................... 3164
  In Errors ........................ 1
  Tunnels .......................... 1
```

Table 37-1: Parameters in the output of the **show l2tp** command

| Parameter | Meaning |
|---|---|
| State | Whether L2TP is enabled. |
| Server | Whether LAC or LNS server mode is enabled, or both. |
| Passwords | Global password and range-limited passwords for authenticating tunnel creation, or "not set" if a password has not been set. |
| Filter | IP filter used to control communication with other L2TP servers, or "none" if a filter has not been set. |
| Default Call Receive Window | The default call receive window size, in packets, that the server tries to negotiate with a remote L2TP server during tunnel creation, or "off" if packet numbering is disabled for L2TP payload packets. The actual call receive window used may differ as a result of the negotiation process. |
| Checksum Payload Packets | Whether checksums are computed for L2TP payload packets. |
| Failed Authentications | Number of times authentication with a remote L2TP server has failed during tunnel creation. |
| In Messages | Number of L2TP packets received by this router. |
| Out Messages | Number of L2TP packets transmitted by this router. |
| In Errors | Number of L2TP packets received by this router which contained errors. |
| Tunnels | Number of L2TP tunnels currently active. |

Figure 37-6: Example output from the **show l2tp counter** command

```
L2TP Server

  State ............................ enabled
  Server ........................... both
  Password ......................... not set
  Filter ........................... not set
  Default Call Receive Window ...... 16
  Checksum Payload Packets ......... on
  Failed Authentications ........... 0
  In Messages ...................... 337
  Out Messages ..................... 282
  In Errors ........................ 0
  In Discarded - Disabled .......... 0
  In Discarded - Filtered .......... 0
  In Discarded - No Such Tunnel .... 0
  In Discarded - No Such Call ...... 0
  Mal Formed Packets ............... 0
  In Control Packets ............... 87
  In Control Packets With Data ..... 76
  In Control Packets No Data ....... 10
  Processed Control Packets ........ 86
  In Order Control Packets ......... 76
  Out Of Order Control Packets ..... 1
  Order Discarded Ctl Packets ...... 1
  Out Control Packets .............. 65
  Out Control Packets With Data .... 36
  Out Control Packets No Data ...... 29
  In Data Packets .................. 250
  In Data Packets With Data ........ 150
  In Data Packets No Data .......... 100
  Processed Data Packets ........... 250
  In Order Data Packets ............ 58
  Out Of Order Data Packets ........ 100
  Order Discarded Data Packets ..... 0
  Out Data Packets ................. 217
  Out Data Packets With Data ....... 178
  Out Data Packets No Data ......... 39
  Tunnels .......................... 1
```

Table 37-2: Parameters in the output of the **show l2tp counter** command

| Parameter | Meaning |
|---|---|
| State | Whether L2TP is enabled. |
| Server | Whether LAC or LNS server mode is enabled, or both. |
| Password | Global password for authenticating tunnel creation or "none" if a password has not been set. |
| Filter | IP filter used to control communication with other L2TP servers, or "none" if a filter has not been set. |
| Default Call Receive Window | The default call receive window size, in packets, that the server wll attempt to negotiate with a remote L2TP server during tunnel creation, or "off" if packet numbering is disabled for L2TP payload packets. The actual call receive window used may differ as a result of the negotiation process. |
| Checksum Payload Packets | Whether checksums are computed for L2TP payload packets. |
| Failed Authentications | Number of times authentication with a remote L2TP server has failed during tunnel creation. |
| In Messages | Number of L2TP packets received by this router. |
| Out Messages | Number of L2TP packets transmitted by this router. |
| In Errors | Number of L2TP packets with errors received by this router. |
| In Discarded - Disabled | Number of L2TP messages discarded because the L2TP server was disabled. |
| In Discarded - Filtered | Number of L2TP messages discarded due to an IP filter match. |
| In Discarded - No Such Tunnel | Number of L2TP messages discarded because the Tunnel ID in the message did not match any active tunnel. |
| In Discarded - No Such Call | Number of L2TP messages discarded because the Call ID in the message did not match an active call. |
| Mal Formed Packets | Number of badly formatted L2TP packets received by the router. |
| In Control Packets | Number of L2TP control packets received by the router. |
| In Control Packets With Data | Number of L2TP control packets with data received by the router. |
| In Control Packets No Data | Number of L2TP control packets without data received by the router. |
| Processed Control Packets | Number of L2TP control packets processed by the router. |
| In Order Control Packets | Number of L2TP control packets received in order by the router. |
| Out Of Order Control Packets | Number of L2TP control packets received out of order by the router. |
| Order Discarded Ctl Packets | Number of L2TP control packets discarded by the router because the packets were received out of order. |
| Out Control Packets | Number of L2TP control packets transmitted by the router. |
| Out Control Packets With Data | Number of L2TP control packets with data transmitted by the router. |
| Out Control Packets No Data | Number of L2TP control packets without data transmitted by the router. |

Table 37-2: Parameters in the output of the **show l2tp counter** command (continued)

| Parameter | Meaning |
|---|---|
| In Data Packets | Number of L2TP payload packets received by the router. |
| In Data Packets With Data | Number of L2TP payload packets with data received by the router. |
| In Data Packets No Data | Number of L2TP payload packets without any data received by the router. |
| Processed Data Packets | Number of L2TP payload packets processed by the router. |
| In Order Data Packets | Number of L2TP payload packets received in order by the router. |
| Out Of Order Data Packets | Number of L2TP payload packets received out of order by the router. |
| Order Discarded Data Packets | Number of L2TP payload packets discarded by the router because the packets were received out of order. |
| Out Data Packets | Number of L2TP payload packets transmitted by the router. |
| Out Data Packets With Data | Number of L2TP payload packets containing data transmitted by the router. |
| Out Data Packets No Data | Number of L2TP payload packets that did not contain any data transmitted by the router. |
| Tunnels | Number of L2TP tunnels currently active. |

**Examples** To display the status of L2TP, use the command:

```
sh l2tp
```

**See Also**
**add l2tp password**
**delete l2tp password**
**disable l2tp**
**disable l2tp debug**
**disable l2tp server**
**enable l2tp**
**enable l2tp debug**
**enable l2tp server**
**set l2tp checksum**
**set l2tp filter**
**set l2tp password**

# show l2tp call

**Syntax** `SHow L2TP CALL[=`*`name`*`]`

where *name* is an L2TP call name 1 to 15 characters long that is not case-sensitive. Valid characters are uppercase and lowercase letters, decimal digits (0–9) and the underscore character ("_").

**Description** This command displays information about the specified call definition or all defined calls (Figure 37-7 on page 37-34, Table 37-3 on page 37-34).

Figure 37-7: Example output from the **show l2tp call** command

```
L2TP Call Information

------------------------------------------------------------
Name : test
  Type ..................... virtual
  Precedence ............... out
  Sequence numbering ...... off
  Remote is pre draft13 ... on
  Speed .................... 64000
  IP address ............... 192.168.1.2
  Password ................. not set
  Remote callname ......... test
  Dial ..................... not set
  Subaddress ............... not set
```

Table 37-3: Parameters in the output of the **show l2tp call** command

| Parameter | Meaning |
|---|---|
| Name | Name of an L2TP call. |
| Type | Type of call the router at the remote end of the L2TP tunnel (acting as a LAC) uses to make the final connection to the remote user; either "async", "isdn", or "virtual". |
| Precedence | Precedence for this call, either "in" or "out". |
| Sequence numbering | Whether L2TP data packets are numbered: "on" (always numbered), "off" (numbered only if the remote end requests sequence numbering), or "startup" (numbered only during the startup sequence). |
| Remote is pre draft13 | Whether the remote L2TP server is a pre-Draft 13 L2TP server. |
| Speed | Maximum bandwidth of the connection in bits per second. |
| IP address | IP address of the remote L2TP server. |
| Password | Password used to authenticate the L2TP tunnel creation with the remote L2TP server |
| Remote callname | Name of the ACC, ISDN or L2TP call on the remote L2TP server that is activated by this L2TP tunnel. |
| Dial | Number to dial to read the remote location, or "not set" if the number has not been set. This is either a PSTN number or an ISDN number, including all access codes and area codes. |
| Subaddress | The ISDN subaddress to use when the Type field is set to "isdn", or "not set". |

**Examples** To display all defined calls, use the command:

```
sh l2tp call
```

**See Also** **activate l2tp call**
**add l2tp call**
**deactivate l2tp call**
**delete l2tp call**
**set l2tp call**

# show l2tp ip

**Syntax** `SHow L2TP IP`

**Description** This command displays the associations between PPP templates and remote L2TP peers (Figure 37-8 on page 37-35, Table 37-4 on page 37-35). When an L2TP call is received from a matching IP address and a dynamic PPP interface is created the associated template is used to configure the interface. This command is only valid on a router acting as an LNS.

Figure 37-8: Example output from the **show l2tp ip** command

```
L2TP IP Range Information
-------------------------------------------------------------
IP Range ....................... 192.168.1.2
  PPP template ................. 1
  Sequence numbering ........... off
  Pre-draft 13 support ......... off
-------------------------------------------------------------
```

Table 37-4: Parameters in the output of the **show l2tp ip** command

| Parameter | Meaning |
|---|---|
| IP Range | IP address or range of IP addresses associated with the PPP template. |
| PPP template | PPP template to use when configuring dynamic PPP interfaces over L2TP calls from L2TP peers with the associated IP address. |
| Sequence numbering | Whether L2TP data packets are numbered: "on" (always numbered), "off" (numbered only if the remote end requests sequence numbering), or "startup" (numbered only during the startup sequence). |
| Pre-draft 13 support | Whether there is compatibility with pre-Draft 13 L2TP servers. |

**Examples** To display the associations between PPP templates and L2TP peers, use the command:

```
sh l2tp ip
```

**See Also** **add l2tp ip**
**delete l2tp ip**

# show l2tp tunnel

**Syntax** `SHow L2TP TUNnel[=`*`tunnelId`*`] [CALL[=`*`callid`*`]] [COUnter]`

where:

- *tunnelId* is the tunnel Id number of a L2TP tunnel from 1 to 65535.
- *callid* is the call ID number of a dynamic call from 1 to 65535.

**Description** This command displays information about the specified tunnel or all currently active tunnels (Figure 37-9 on page 37-36, Table 37-5 on page 37-37). If CALL is specified with a value, detailed information is displayed about the specified active call (Figure 37-10 on page 37-38, Table 37-6 on page 37-38). If CALL is specified without a value, summary information is displayed about all currently active calls.

The COUNTER parameter displays detailed counters for the specified tunnel, all currently active tunnels (Figure 37-11 on page 37-41, Table 37-7 on page 37-41), or the specified call (Figure 37-12 on page 37-42, Table 37-8 on page 37-42).

Figure 37-9: Example output from the **show l2tp tunnel** command

```
Tunnel ID ..................... 3
  State ....................... established
  Started ..................... 08-Apr-1998 11:04:50
  Debug ....................... disabled
  Receive Window .............. 4
  Remote IP Address ........... 192.168.20.1
  Remote UDP Port ............. 1701
  Remote Tunnel ID ............ 2
  Remote Receive Window ....... 4
  Remote Firmware ............. 7-4
  Remote Framing .............. sync+async
  Remote Bearer ............... digital+analog
  Remote Hostname ............. M-L2TP-7-B
  Max Timeout (s ) ............ 15
  Round Time Trip ............. 29
  Adaptive Time-Out ........... 45
  Last Acked .................. 51
  Next Sent ................... 51
  Next Received ............... 51
  Calls Active ................ 1
    Call ID ..................... 3
    Server Type ................. LNS
    Started ..................... 08-Apr-1998 11:04:50
    Username .................... not set
    State ....................... established
    Call Serial Number .......... 3
    Remote Call ID .............. 2
```

Table 37-5: Parameters in the output of the **show l2tp tunnel** command

| Parameter | Meaning |
|---|---|
| Tunnel ID | Tunnel identification number assigned to this tunnel by this router. |
| State | Current state of the tunnel; either "idle", "wait-ctl-reply", "wait-ctl-conn", "wait-reply", "established", or "illegal". |
| Started | Date and time the tunnel was created. |
| Debug | Whether debugging is enabled for this tunnel. If enabled, whether "state", "packet", or "illegal". |
| Debug Device | Device where debug output is sent. |
| Receive Window | The receive window size, in packets, for the L2TP server at this end of the tunnel. |
| Remote IP address | IP address of the L2TP server at the remote end of the tunnel. |
| Remote UDP Port | UDP port used by the tunnel on the remote L2TP server. |
| Remote Tunnel ID | Tunnel identification number for this tunnel on the remote L2TP server. |
| Remote Receive Window | The receive window size, in packets, for the L2TP server at the remote end of the tunnel. |
| Remote Firmware | Firmware (software release) running on the L2TP server at the remote end of the tunnel. |
| Remote Framing | Framing used by the remote L2TP server for the connection to the final destination; either "none", "sync", "async", or "sync+async". |
| Remote Bearer | The bearer used by the remote L2TP server for the connection to the final destination; either "none", "digital", "analog", or "digital+analog". |
| Remote Hostname | Host name of the remote L2TP server. If the remote L2TP server is an AR400 Series router, this is the router's system name set with the **set system name** command on page 1-124 of Chapter 1, Operation. |
| Max Timeout (s) | Maximum round trip time, in tenths of a second, allowed for L2TP traffic on this tunnel. |
| Round Trip Time | Current average round trip time, in tenths of a second, allowed for L2TP traffic on this tunnel. |
| Adaptive Time-Out | Time interval, in tenths of a second, allowed for acknowledgements to be returned. |
| Last Acked | The packet number of the last L2TP payload packet that has been received and acknowledged. |
| Next Sent | The send number to be used in the next L2TP payload packet to be transmitted. |
| Next Received | The receive number expected in the next L2TP payload packet to be received. |
| Calls Active | Number of currently active L2TP calls on this tunnel. |
| Call ID | Call identification number for an active call. |
| Server Type | Whether the server mode for this call is LAC or LNS. |
| Started | Date and time the call was initiated. |
| Username | Username associated with this call. |

Table 37-5: Parameters in the output of the **show l2tp tunnel** command (continued)

| Parameter | Meaning |
|---|---|
| State | Whether the call is idle, wait-cs-answer, wait-connect, or established. |
| Call Serial Number | Unique identifier for this call, assigned by the LAC. |
| Remote Serial Number | Unique identifier for this call, assigned by the remote L2TP server if the remote L2TP server initiated the call. |
| Remote Call ID | Call identification number for this call on the remote L2TP server. |

Figure 37-10: Example output from the **show l2tp tunnel** command for a specific active call

```
Call ID ......................... 3
  Server Type ..................... LNS
  Started ......................... 08-Apr-1998 11:04:50
  Username ........................ not set
  State ........................... established
  Debug ........................... disabled
  Call Serial Number .............. 3
  Remote Call ID .................. 2
  Authentication Type ............. 4
  Remote Receive Window ........... 16
  Processing Delay ................ 10
  Physical Channel ................ 0
  Framing ......................... sync
  Bearer .......................... digital
  Connect Speed ................... 0
  Dialed Number ................... not set
  Sub-Address ..................... head-user1
  Private Group ID ................ not set
  Round Time Trip ................. 19
  Adaptive Time-Out ............... 35
  Last Acked ...................... 3056
  Unacked ......................... 1
  Received Unacked ................ 1
  Force Ack Window ................ 2
  Current Window .................. 16
  Tx Queue Length ................. 1
  Next Sent ....................... 3057
  Next Received ................... 3056
  In Discards ..................... 4
  In Packets ...................... 3056
  In Bytes ........................ 866722
  Out Packets ..................... 3137
  Out Bytes ....................... 867970
```

Table 37-6: Parameters in the output of the **show l2tp tunnel** command for a specific active call

| Parameter | Meaning |
|---|---|
| Call ID | Call identification number for an active call. |
| Server Type | Whether the server mode for this call is LAC or LNS. |
| Started | Date and time the call was initiated. |
| Username | Username associated with this call. |

Table 37-6: Parameters in the output of the **show l2tp tunnel** command for a specific active call (continued)

| Parameter | Meaning |
|---|---|
| State | Whether the status of the call is idle, wait-cs-answer, wait-connect, or established. |
| Debug | Whether debugging is enabled for this tunnel. If enabled, whether "state", "packet", or "illegal". |
| Debug Device | Device where debug output is sent. |
| Call Serial Number | Unique identifier for this call, assigned by the LAC. |
| Remote Call ID | Call identification number for this call on the remote L2TP server. |
| Authentication Type | Proxy authentication type. |
| Remote Receive Window | The receive window size, in packets, for the L2TP server at the remote end of the tunnel. |
| Processing Delay | Time in tenths of a second exchanged during the call control phase. |
| Physical Channel | Remote physical channel number used for the call. The meaning is vendor-specific. |
| Framing | Framing to be used by the remote L2TP server for the connection to the final destination; either "none", "sync", "async", or "sync+async". |
| Bearer | Bearer to be used by the remote L2TP server for the connection to the final destination; either "none", "digital", "analog", or "digital+analog". |
| Connect Speed | Speed requested for the remote connection. |
| Dialed Number | Number to dial to reach the remote location, or "not set" if the number has not been set. This is either a PSTN number or an ISDN number, including all access codes and area codes. |
| Subaddress | ISDN subaddress to use when the Dialed Number field contains an ISDN number, or "not set". |
| Private Group ID | Number used to associate the call with a particular customer group. |
| Remote Processing Delay | Time value requested by the remote L2TP server, in tenths of a second, exchanged during the call control phase. |
| Remote Physical Channel | Remote physical channel number requested by the remote L2TP server to used for the call. The meaning is vendor-specific. |
| Remote Framing | Framing requested by the remote L2TP server to be used for the local connection to the final destination; either "none", "sync", "async", or "sync+async". |
| Remote Bearer | Bearer requested by the remote L2TP server to be used for the local connection to the final destination; either "none", "digital", "analog", or "digital+analog". |
| Remote Connect Speed | Speed requested by the remote L2TP server for the local connection. |
| Remote Dialed Number | Number passed by the remote L2TP server to dial to reach the local destination, or "not set" if the number has not been set. This is either a PSTN number or an ISDN number, including all access codes and area codes. |

Table 37-6: Parameters in the output of the **show l2tp tunnel** command for a specific active call (continued)

| Parameter | Meaning |
|---|---|
| Remote Sub-Address | ISDN subaddress passed by the remote L2TP server to use when the Dialed Number field contains an ISDN number, or "not set". |
| Remote Private Group ID | Number passed by the remote L2TP server used to associate the call with a particular customer group. |
| Round Trip Time | Current average round trip time, in seconds, allowed for L2TP traffic on this call. |
| Adaptive Time-Out | Time interval, in tenths of a second, allowed for acknowledgements to be returned. |
| Last Acked | Packet number of the last L2TP payload packet for this call that has been received and acknowledged. |
| Unacked | Number of L2TP payload packets for this call that have been transmitted for which an acknowledgement has not yet been received from the remote L2TP server. |
| Received Unacked | Number of L2TP payload packets for this call that have been received but not yet acknowledged. |
| Force Ack Window | Number of packets received before an acknowledgement is transmitted. |
| Current Window | The receive window size, in packets, for the L2TP server at this end of the tunnel. |
| Tx Queue Length | Number of packets waiting to be transmitted over the tunnel for this call. |
| Next Sent | The send number to be used in the next L2TP payload packet to be transmitted for this call. |
| Next Received | The receive number expected in the next L2TP payload packet to be received for this call. |
| In Discards | Number of incoming L2TP payload packets that were discarded because they contained an error. |
| In Packets | Number of L2TP payload packets received for this call. |
| In Bytes | Number of bytes of payload received for this call. |
| Out Packets | Number of L2TP payload packets transmitted for this call. |
| Out Bytes | Number of bytes of payload transmitted for this call. |

Figure 37-11: Example output from the **show l2tp tunnel counter** command

```
Tunnel ID ..................... 12
  State ....................... established
  Started ..................... 21-Apr-1998 05:13:39
  Remote IP Address ........... 192.168.72.78
  Remote UDP Port ............. 1701
  Remote Tunnel ID ............ 304
  Remote Hostname ............. NAC
  In Control Packets .............. 5
  In Control Packets With Data .... 5
  In Control Packets No Data ...... 0
  Processed Control Packets ....... 6
  In Order Control Packets ........ 6
  Out Of Order Control Packets .... 0
  Order Discarded Ctl Packets ..... 0
  Out Control Packets ............. 5
  Out Control Packets With Data ... 3
  Out Control Packets No Data ..... 2
  Out Flow Control Timeouts ....... 0
```

Table 37-7: Parameters in the output of the **show l2tp tunnel counter** command

| Parameter | Meaning |
|---|---|
| Tunnel ID | Tunnel identification number assigned to this tunnel by this router. |
| State | Current status of the tunnel; either “idle”, “wait-ctl-reply”, “wait-ctl-conn”, “wait-reply”, “established”, or “illegal”. |
| Started | Date and time the tunnel was created. |
| Remote IP address | IP address of the L2TP server at the remote end of the tunnel. |
| Remote UDP Port | UDP port used by the tunnel on the remote L2TP server. |
| Remote Tunnel ID | Tunnel identification number for this tunnel on the remote L2TP server. |
| Remote Hostname | Host name of the remote L2TP server. If the remote L2TP server is an AR400 Series router, this is the router’s system name set with the **set system name** command on page 1-124 of Chapter 1, Operation. |
| In Control Packets | Number of L2TP control packets received over this tunnel. |
| In Control Packets With Data | Number of L2TP control packets containing data received over this tunnel. |
| In Control Packets No Data | Number of L2TP control packets that did not contain any data received over this tunnel. |
| Processed Control Packets | Number of L2TP control packets received over this tunnel that were processed by the router. |
| In Order Control Packets | Number of L2TP control packets received in order over this tunnel. |
| Out Of Order Control Packets | Number of L2TP control packets received out of order over this tunnel. |
| Order Discarded Ctl Packets | Number of L2TP control packets received over this tunnel that were discarded because the packets were received out of order. |

Table 37-7: Parameters in the output of the **show l2tp tunnel counter** command

| Parameter | Meaning |
|---|---|
| Out Control Packets | Number of L2TP control packets transmitted over this tunnel. |
| Out Control Packets With Data | Number of L2TP control packets containing data transmitted over this tunnel. |
| Out Control Packets No Data | Number of L2TP control packets that did not contain any data transmitted over this tunnel. |
| Out Flow Control Timeouts | Number of L2TP control timeout packets transmitted over this tunnel. |

Figure 37-12: Example output from the **show l2tp tunnel call counter** command

```
Call ID ......................... 32760
 Tunnel ID ...................... 19968
 Server Type .................... LAC
 Started ........................ 11-Sep-2003 11:29:37
 Username ....................... not set
 State .......................... idle
 Call Serial Number ............. 3
 Remote Call ID ................. 0
 In Packets ..................... 0
 In Bytes ....................... 0
 In Payload Packets ............. 0
 In Payload Packets With Data .... 0
 In Payload Packets No Data ..... 0
 Processed Payload Packets ...... 0
 In Order Payload Packets ....... 0
 Out Of Order Payload Packets .... 0
 Order Discarded Packets ........ 0
 In Discards .................... 0
 Out Packets .................... 0
 Out Bytes ...................... 0
 Out Payload Packets ............ 0
 Out Payload Packets With Data ... 0
 Out Payload Packets No Data ..... 0
 Out Flow Payload Timeouts ...... 0
```

Table 37-8: Parameters in the output of the **show l2tp tunnel call counter** command

| Parameter | Meaning |
|---|---|
| Call ID | Call identification number for an active call. |
| Tunnel IDs | Tunnel identification number assigned to this tunnel by this router. |
| Server Type | Whether the server mode for this call is LAC or LNS. |
| Started | Date and time the call was initiated. |
| Username | Username associated with this call. |
| State | Whether the status of the call is idle, wait-cs-answer, wait-connect, or established. |
| Call Serial Number | Unique identifier for this call assigned by the LAC. |
| Remote Serial Number | Unique identifier for this call assigned by the remote L2TP server if the remote L2TP server initiated the call. |

Table 37-8: Parameters in the output of the **show l2tp tunnel call counter** command

| Parameter | Meaning |
|---|---|
| Remote Call ID | Call identification number for this call on the remote L2TP server. |
| In Packets | Number of L2TP packets received over this call. |
| In Bytes | Number of bytes of data received over this call. |
| In Payload Packets | Number of L2TP payload packets received over this call. |
| In Payload Packets With Data | Number of L2TP payload packets containing data received over this call. |
| In Payload Packets No Data | Number of L2TP payload packets that did not contain any data received over this call. |
| Processed Payload Packets | Number of L2TP payload packets received over this call that were processed by the router. |
| In Order Payload Packets | Number of L2TP payload packets received in order over this call. |
| Out Of Order Payload Packets | Number of L2TP payload packets received out of order over this call. |
| Order Discarded Packets | Number of L2TP payload packets received over this call that were discarded because the packets were received out of order. |
| In Discards | Number of L2TP payload packets received over this call that were discarded. |
| Out Packets | Number of L2TP packets transmitted over this call. |
| Out Bytes | Number of bytes of data transmitted over this call. |
| Out Payload Packets | Number of L2TP payload packets transmitted over this call. |
| Out Payload Packets With Data | Number of L2TP payload packets containing data transmitted over this call. |
| Out Payload Packets No Data | Number of L2TP payload packets that did not contain any data transmitted over this call. |
| Out Flow Payload Timeouts | Number of L2TP payload timeouts occurring during transmission. |

**Examples** To show all calls active on the tunnel with ID 3, use the command:

```
sh l2tp tun=3
```

To show counters for all active tunnels, use the command:

```
sh l2tp tun cou
```

To show counters for call ID 36 on tunnel ID 12, use the command:

```
sh l2tp tun=12 call=36 cou
```

**See Also**

activate l2tp call
add l2tp call
add l2tp password
deactivate l2tp call
delete l2tp call
delete l2tp user
set l2tp call
set l2tp user
show l2tp
show l2tp call

# show l2tp user

**Syntax** `SHow L2TP USer=[`*`mapping`*`]`

where *mapping* is a structured username string of printing characters from 1 to 63 characters long

**Description** This command is used to display attributes of a single defined user mapping entry, or if the mapping is not set, the attributes of all defined user mapping entries.

Figure 37-13: Example output from the **show l2tp user** command

```
L2TP User Information
-------------------------------------------------------------
User : dataman
  Action ................... database
  Password ................. not set
  Maximum timeout .......... 20
  Sequence Numbering ....... on
  Remote is pre draft13 .... on
  Remote IP ................ 192.168.1.2
  Remote Port .............. 1701

User : anothemap
  Action ................... dnslookup
  Password ................. userpass
  Maximum timeout .......... 20
  Sequence Numbering ....... off
  Remote is pre draft13 .... off
  Prefix ................... uname

User : ispname
  Action ................... radius
  Password ................. not set
  Maximum timeout .......... 15
  Sequence Numbering ....... off
  Remote is pre draft13 .... off
```

Table 37-9: Parameters in the output of the **show l2tp user** command

| Parameter | Meaning |
|---|---|
| User | PPP username to match for this map entry; either "all", "local", "none", "remote", or a structured username. |
| Action | Action to take when a PPP username matches this map entry; either "database", "dnslookup", "ignore", or "radius". |
| Password | Password to use when authenticating the tunnel creation to the remote L2TP server. |
| Maximum timeout | When set, maximum round trip time, in seconds, for L2TP traffic. |
| Sequence numbering | Whether L2TP data packets are numbered: "on" (always numbered), "off" (numbered only if the remote end requests sequence numbering), or "startup" (numbered only during the startup sequence). |
| Remote is pre draft13 | Whether the remote L2TP server is a pre-Draft 13 L2TP server. |
| Remote IP | IP address of the remote L2TP server. Valid only when the Action field is set to **database**. |
| Remote Port | UDP port on the remote L2TP server. Valid only when the Action field is set to **database**. |
| Prefix | Prefix to apply to the domain name portion of the User field for DNS lookups. Valid only when the Action field is set to **dnslookup**. |

**Examples** To show all the user mappings defined, use the command:

```
sh l2tp us
```

**See Also**
**add l2tp user**
**delete l2tp user**
**set l2tp user**
**show l2tp**