Chapter 20

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

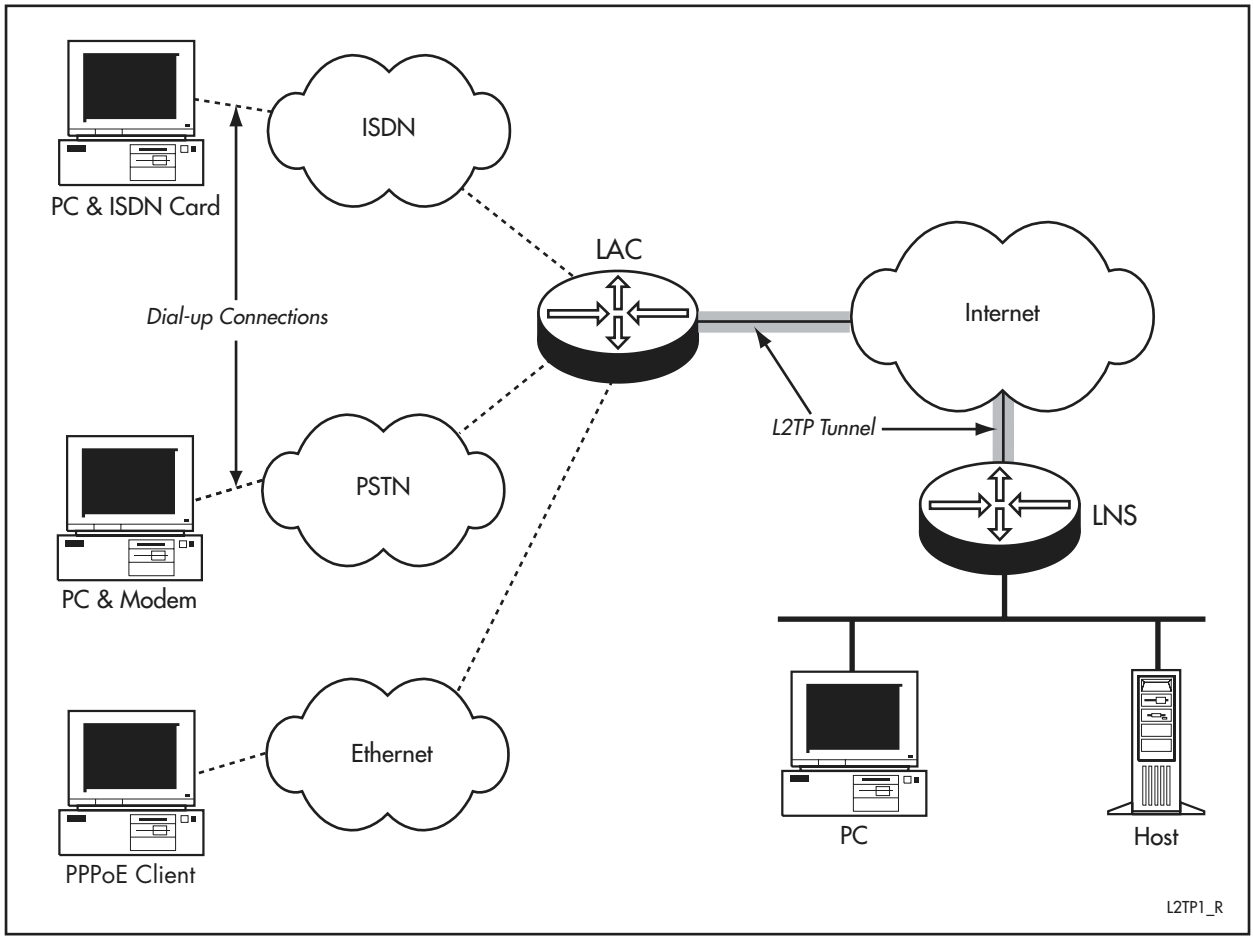
L2TP creates a tunnel across the Internet between an L2TP Access Concentrator (LAC) and an L2TP Network Server (LNS). This enables Point-to-Point Protocol (PPP) link layer frames to be encapsulated and carried across the Internet (Figure 20-1 on page 20-4). A remote user initiates a dial-up PPP connection to an *Internet Service Provider* (ISP) via a PSTN, ISDN or Ethernet service. The LAC accepts the connection and a local 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, the LAC creates an L2TP tunnel (or uses an existing tunnel if one exists) to the desired LNS. An unused slot within the tunnel, known as a "call", 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 this 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 through the tunnel. The LAC strips the CRC, link framing and transparency bytes from the locally received frames, encapsulates them in L2TP and forwards them through the tunnel. At the remote end of the tunnel, the LNS accepts the frames, strips off the L2TP encapsulation and processes them 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 20-1: 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.

Overview of L2TP on the Router

The router implements L2TP as defined in RFC 2661, *Layer Two Tunnelling Protocol (L2TP)*. It can act as both an L2TP Access Concentrator (LAC) and an L2TP Network Server (LNS).

The router's L2TP implementation enables it to:

- receive inbound ACC, ISDN, and PPPoE calls and create a L2TP tunnel to the desired LNS
- create outbound ACC calls as an LAC on behalf of an LNS
- create outbound ISDN calls as an LAC on behalf of an LNS
- receive and create L2TP calls as an LNS
- create virtual tunnels with L2TP peers
- reflect a packet's original QoS information into the L2TP header
- use a RADIUS or DNS server, or the L2TP user database, to determine which LNS a dial-up session is tunnelled to
- use IP address filtering to allow only L2TP traffic from specific remote L2TP servers

When an ACC call, ISDN call, or PPPoE session connects to the router, a temporary dynamic PPP interface is created, which is used to negotiate the connection, and determine the dial-up user's login name. The router uses the login name to determine whether to create an L2TP tunnel to an LNS, or to terminate the PPP session locally. The router terminates the PPP session locally for other session types, such as when the user wants an Internet session created. If the router determines it should create a tunnel to a remote LNS server, L2TP takes control of the lower layer interface. This makes redundant the temporary PPP interface with the user, so it is terminated.

When a tunnel is needed, the router sends a request to the LNS to establish an L2TP tunnel. Once a tunnel is established, the LNS authenticates directly with the remote user. The LNS uses a PPP template to configure and authenticate the main PPP link between itself and the remote user.

When the router and the LNS have a tunnel already established, the call uses the established tunnel, as multiple calls can travel through the same tunnel.

The LAC and the LNS both use PPP templates when handling incoming calls. The PPP template parameters do not have to be the same on the LAC and LNS. See Chapter 15, Point-to-Point Protocol (PPP) for more information about PPP and creating PPP templates.

Before the router, acting as a LAC, can accept an incoming call, it must have a call defined to answer the dial-up connection. To define a call, see the appropriate chapter:

- See Chapter 19, Asynchronous Call Control for detailed information about defining an ACC call.
- See Chapter 11, Integrated Services Digital Network (ISDN) for detailed information about defining an ISDN call.

Enabling L2TP on the Router

L2TP is disabled by default. Before the router can act as an LAC or LNS server, L2TP must be globally enabled on the router. Use the command:

```
enable l2tp
```

To globally disable L2TP, using the command:

```
disable l2tp
```

The router has the LAC and LNS server modes disabled by default. To enable these, use the command:

```
enable l2tp server={both|lac|lns}
```

Selecting **both** will enable both the LNS and the LAC server on the router. To disable the servers, use the command:

```
disable l2tp server={both|lac|lns}
```

To display the global configuration and status of L2TP, use the command:

```
show l2tp
```

You can restrict the range of remote L2TP servers the router can communicate with by associating an IP filter to L2TP. An IP filter must first be created using the **add ip filter** command on page 22-70 of Chapter 22, Internet Protocol (IP). Once you have created the IP filter, associate the filter to the router's L2TP servers by using the command:

```
set l2tp filter={0..299|none}
```

Accepting Incoming Calls as an LAC

The router needs to be configured as an LAC server to accept incoming ACC calls, ISDN calls, or PPPoE sessions and redirect them over an L2TP tunnel. Use the command:

```
enable l2tp server=lac
```

Before L2TP can act on an incoming call, the router must have a call defined to answer the dial-up connection. To define a call, see the appropriate chapter:

- See Chapter 19, Asynchronous Call Control for detailed information about defining an ACC call.
- See Chapter 11, Integrated Services Digital Network (ISDN) for detailed information about defining an ISDN call.

The router must have L2TP user mappings configured before it can create an L2TP tunnel to a remote LNS. The router uses the user mapping to decide what action occurs to the call. To create a user mapping, use the command:

```
add l2tp user={mapping|all|local|none|remote}
    action={database|dnslookup|ignore|radius}
    [ip=ipadd [port=1..65535]] [number={off|on}]
    [password=password] [pre13={on|off}]
    [prefix=prefix] [timeout=8..300]
    [tosreflect={off|on|false|true|no|yes}]
```

The user mappings are modified using the command:

```
set l2tp user={mapping|all|local|none|remote} [other-options]
```

If a user connects with a username matching a map entry with an **action** of **ignore**, L2TP ignores the call and the router creates a normal Internet connection. Any other action causes L2TP to create an L2TP tunnel. The other **action** parameter options determines how L2TP retrieves the information it needs to create the tunnel, such as the IP address of the remote L2TP server. When **database** is specified, the ip address, and optionally the port number, of the remote LNS must be specified in the user mapping.

To display information about the currently defined user mappings, use the command:

```
show l2tp user[=mapping]
```

To delete a username mapping, use the command:

```
delete l2tp user={mapping|all|local|none|remote}
```

Accepting L2TP Sessions as an LNS

The router needs to be configured as an LNS server to accept incoming L2TP sessions from remote LACs. Use the command:

```
enable l2tp server=lns
```

The router must have a PPP template defined before it can act on an L2TP session request from an LAC. The router uses the PPP template to configure the dynamic PPP interface created between itself and the LAC. See Chapter 15, Point-to-Point Protocol (PPP) for detailed information about configuring PPP templates.

The router identifies an incoming call from an LAC using the LAC's IP address. To associate a PPP template and other call attributes to an IP address or IP address range, use the command:

```
add l2tp ip={ipadd|ipadd-ipadd} ppptemplate=0..31
    [number={off|on|startup}] [pre13={off|on}]
    [proxyauth={off|on}]
    [tosreflect={off|on|false|true|no|yes}]
```

When the LNS receives a call from an LAC with an IP address that matches an IP entry, the router creates a dynamic PPP interface over the L2TP tunnel. It does this by using the PPP template specified by the **ppptemplate** parameter to configure the PPP interface.

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. The **number** parameter determines how the LNS handles data packet sequence numbering for the call.

To display the current associations between IP addresses and PPP templates, use the command:

```
show l2tp ip
```

To remove the association between an IP address and a PPP template, use the command:

```
delete l2tp ip={ipadd|ipadd-ipadd}
```

Linking Passwords to Incoming Sessions

You can associate a password with LACs by designating a password to an IP address range. Use the command:

```
add l2tp password={password|none} [ip={ipadd|ipadd-ipadd}
```

If the IP address of the LAC exists in more than one password range on the LNS, then the LNS uses the password that matches the smallest IP range. If there are IP ranges of equal size, then the router uses the range with the lowest base IP address.

To display the L2TP passwords configured for the LAC connections to the router, use the command:

```
show l2tp
```

To delete a password associated with an IP range, use the command:

```
delete l2tp password [ip={ipadd|ipadd-ipadd|all}]
```

When **all** is specified, the router deletes all the L2TP passwords except the global password set using the **set l2tp password** command.

Creating a Call from an LNS to an LAC

In a typical scenario, L2TP supports only one-way dial-up connections. That is, a remote user connects to an ISP to start an L2TP session. Once the connection is made, data is 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 out to the user. Only PSTN and ISDN support two-way dial-up connections.

If you require two-way dial-up connections, 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 command:

```
add l2tp call=name ip=ipadd type={async|isdn|virtual}
    [dial=number] [number={off|on|startup}]
    [password=password] [pre13={off|on}] [precedence={in|out}]
    [remotecall=name]  [speed=300..4294967295]
    [subaddress=subaddress]
    [tosreflect={off|on|false|true|no|yes}]
```

To modify an existing call definition, use the command:

```
set l2tp call=name [ip=ipadd] [type={async|isdn|virtual}]
    [dial=number] [other-options]
```

The **type** parameter specifies the type of ACC or ISDN call the LAC uses to make the final connection to the remote user. You can use the **virtual** option to create inter-router tunnels; see the section "Creating an Inter-Router Tunnel" on page 20-9 for further information.

The **remotecall** parameter specifies the name of the call, and must identify an ACC or ISDN call already defined on the LAC. To create a call on the router when it is acting as an LAC, see the appropriate chapter:

- For detailed information about defining an ACC call, see Chapter 19, Asynchronous Call Control.
- For detailed information about defining an ISDN call, see Chapter 11, Integrated Services Digital Network (ISDN).

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

To display information about calls defined on the router, use the command:

```
show l2tp call[=name]
```

To manually activated a call from the LNS, use the command:

```
activate l2tp call=name
```

To deactivate an active L2TP call, use the command:

```
deactivate l2tp call={name|1..65535}
```

To delete an L2TP call, use the command:

```
delete l2tp call=name
```

Creating an Inter-Router Tunnel

You can configure an inter-router tunnel on the router to create a static PPP interface at each end of the L2TP tunnel. To do so, the **type** parameter must be set to **virtual**, and 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 also 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 you require a virtual L2TP call 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.

Monitoring L2TP Connections

To display the global configuration and status of L2TP, and general counters for L2TP, use the command:

```
show l2tp counter
```

To reset the counters displayed by the **show l2tp counter** command, use the command:

```
reset l2tp counter
```

You can monitor the current status of active L2TP tunnels using the **show l2tp tunnel** command. This includes details about the remote connection and a summary of the active calls on each tunnel. Use the command:

```
show l2tp tunnel[=1..65535]
```

To display packet counters useful for monitoring a tunnel, or all tunnels, use the command:

```
show l2tp tunnel counter
```

You can view details about active calls using the **show l2tp tunnel call** command. This includes details about username associated with the call, the type of server the router is acting as for the call, and the connection status of the call. Use the command:

```
show l2tp tunnel call[=1..65535]
```

To display packet counters useful for monitoring a call, or all calls, use the command:

```
show l2tp tunnel call counter
```

Debugging L2TP Connections

You can enable debugging on a per-call or per-tunnel basis, or on all calls and tunnels. Debugging is disabled by default. To enable debugging, use the command:

```
enable l2tp debug={all|decode|pkt|state}
   [call[=1..65535]|tunnel[=1..65535]] [timeout=1..300]
```

To disable debugging for L2TP, use the command:

```
disable l2tp debug={all|decode|pkt|state}
   [call[=1..65535]|tunnel[=1..65535]]
```

The **pkt** option displays payload and control packet data in hexadecimal format. An alternative to **pkt** is **decode**, which displays control messages and payload message headers in a human-readable format. The **state** option displays state changes for both tunnels and calls.

You can set a time limit for how long L2TP debugging occurs by using the **timeout** parameter. Once the limit is reached, the router automatically disables all debugging modes for all calls and tunnels. If you do not set this parameter, then any debugging options enabled will produce debugging information until you explicitly turn them off by using the **disable l2tp debug** command.

Handling PPP Link Negotiation Failures

The connection between the router, acting as an LNS, and a third party peer, acting as an LAC, can sometimes fail during PPP link negotiation. Frequent negotiation failures may indicate a compatibility problem between the third party peer and Proxy Authentication responses from the router. You can disable Proxy Authentication on the router for situations where the third party equipment is not compatible, using **proxyauth=off** in the command:

```
add l2tp ip={ipadd|ipadd-ipadd} ppptemplate=0..31
    [proxyauth={off|on}] [other-options]
```

The default for **proxyauth** is **on**. Proxy Authentication should not be disabled unless necessary. You can use the **show l2tp ip** command to confirm whether Proxy Authentication is on or off.

Reflecting TOS onto L2TP-Tunnelled Packets

Networking equipment uses the TOS/DSCP field of IP packets to carry Quality of Service (QoS) information within a Virtual Private Network (VPN). L2TP normally encapsulates a packet with a new L2TP IP header with a default value of zero in the TOS/DSCP field. This means that appropriate QoS does not occur on the encapsulated packets.

The **tosreflect** parameter allows you to reflect an IP packet's original TOS/DSCP field onto the outer L2TP IP header. This allows networking equipment to apply QoS to the encapsulated packet in the same way it would to the original packet.

You can enable this feature for particular calls by using one of the commands:

```
add l2tp call=name [tosreflect={on|off|yes|no|true|false}]
    [other-options]
```

```
set l2tp call=name [tosreflect={on|off|yes|no|true|false}]
    [other-options]
```

On the LNS server, you can enable this feature for particular IP addresses by using the command:

```
add l2tp ip={ipadd|ipadd-ipadd} ppptemplate=ppp-template
    [tosreflect={on|off|yes|no|true|false}] [other-options]
```

On the LAC server, you can enable this feature for particular dial-up users by using one of the commands:

```
add l2tp user={mapping|all|local|none|remote}
    [tosreflect={on|off|yes|no|true|false}] [other-options]
```

```
set l2tp user={mapping|all|local|none|remote}
    [tosreflect={on|off|yes|no|true|false}] [other-options]
```

Configuration Examples

Examples in this section show the following configurations:

- **Inter-Router Tunnels**
- **Simple Dial-In System**
- **Configure L2TP to Tunnel PPPoE Sessions**

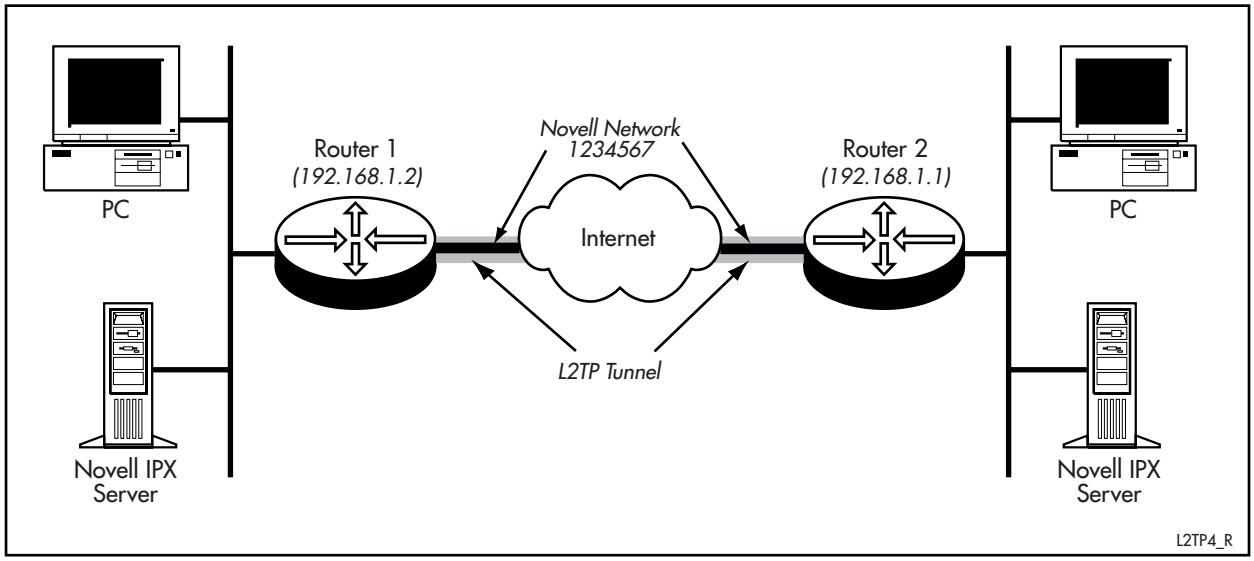
The following documents describe more solutions, and are available from the Resource Center on your Documentation and Tools CD-ROM or from www.alliedtelesis.co.uk/en-gb/solutions/techdocs.asp?area=howto.

- *How To Configure Allied Telesis and Cisco routers to interoperate over L2TP*
- *How To Configure Dynamic Routing Over an L2TP Tunnel*

Inter-Router Tunnels

This 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 20-2).

Figure 20-2: Configuration for inter-router L2TP tunnels



To configure Router 1

1. **Enable the router as both an 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 an 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
```

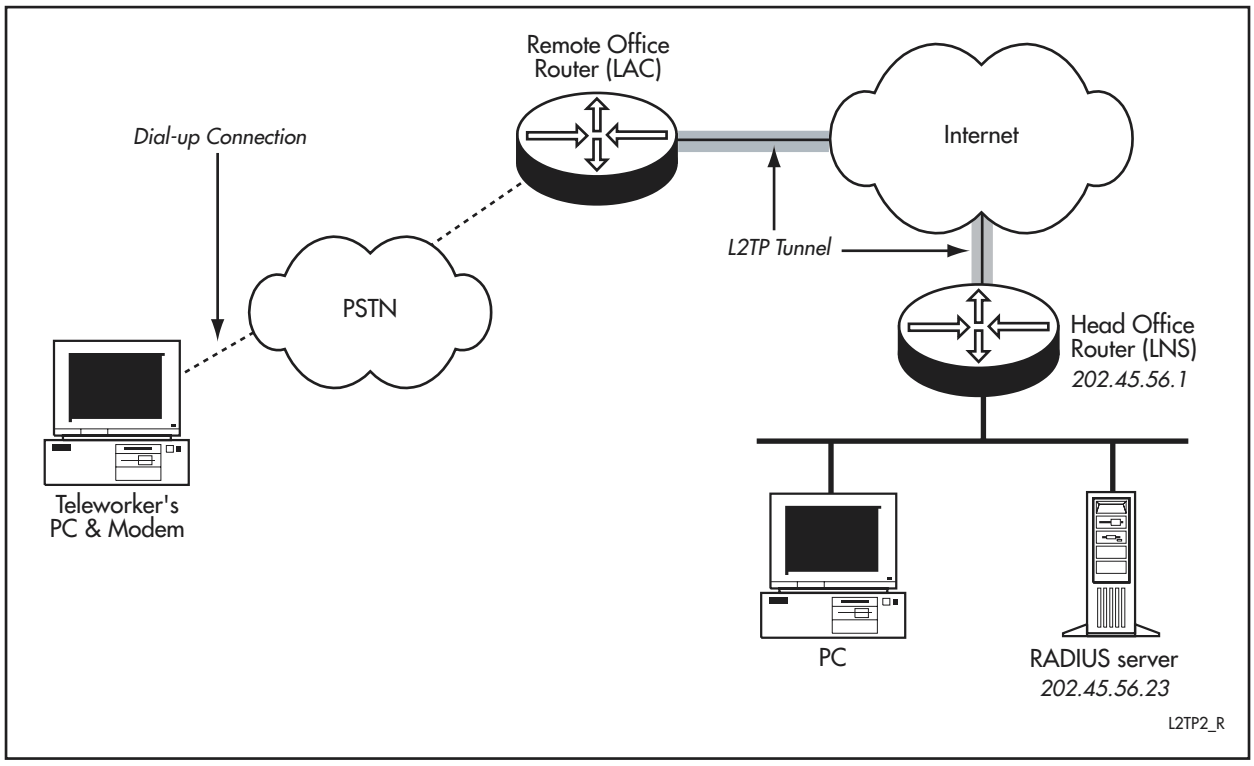
IPX traffic destined for the IPX network 1234567 causes an L2TP tunnel to be created to Router 2.

Simple Dial-In System

This example shows how 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 an 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 20-3).

Figure 20-3: 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.

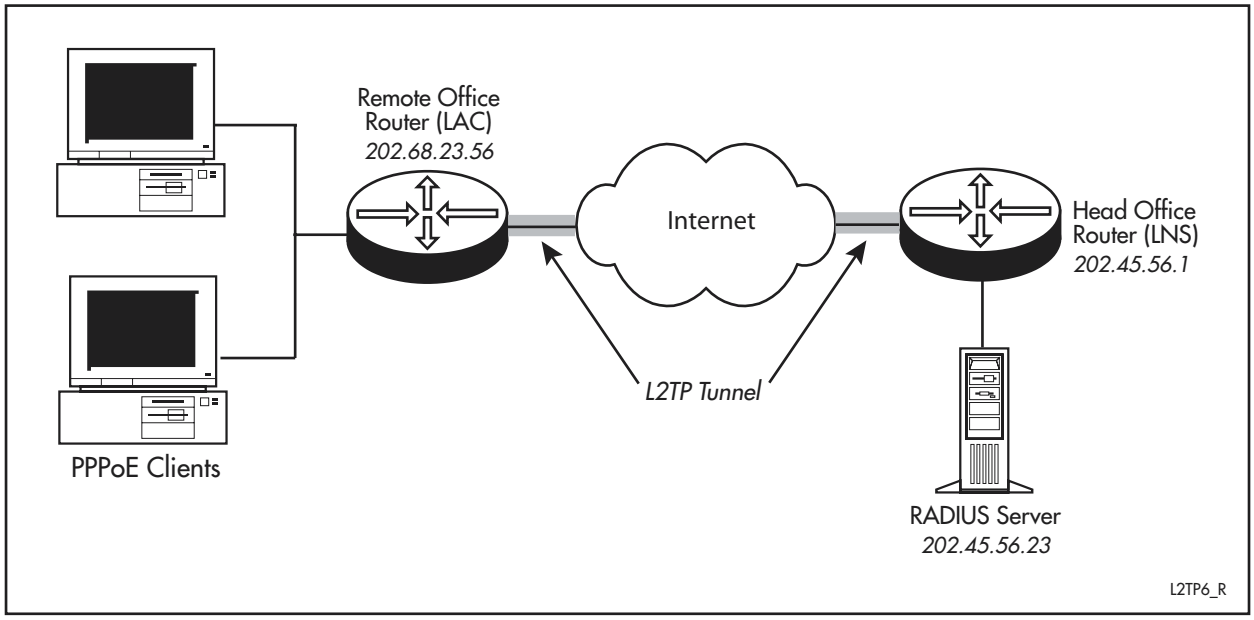
Add a map entry to match the PPP usernames of the teleworkers, and activate an L2TP tunnel to the head office LNS with the IP address 202.45.56.1. Users are authenticated at the head office site using RADIUS:

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

Configure L2TP to Tunnel PPPoE Sessions

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 an LAC. The head office router acts in L2TP terms as an LNS. Users are authenticated at the head office site using RADIUS (Figure 20-4).

Figure 20-4: 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 an L2TP LAC server.

Configure the remote office router to act as an 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 22, 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 lxv of About this Software Reference 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`*

Description This command activates an L2TP call previously defined using the **add l2tp call** command on page 20-19. The L2TP call *name* is between 1 to 15 characters, can be composed of any printable character, but cannot be made entirely of digits (0-9). The name is not case-sensitive.

Using the predefined call information, an L2TP Session (Call) is established to the remote L2TP server. If an L2TP tunnel already exists to the remote server then the new session occurs inside that tunnel. If no tunnel exists then a new tunnel is established. The specified 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 IP=ipadd TYpe={ASYNc|ISDN|VIrtual}
   [DIAL=number] [NUMber={OFF|ON|STARTup}]
   [PASSword=password] [PRE13={OFF|ON}]
   [PRECedence={IN|OUT}] [REMotecall=name]
   [SPeed=300..4294967295] [SUBAddress=subaddress]
   [TOSreflect={OFF|ON|False|True|NO|YES}]
```

Description

This command adds a new 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 uses an existing L2TP tunnel, to the remote location.

Parameter	Description	
CALL	The name of the L2TP call to add. An L2TP call with the same name must not exist. The *name* must be between 1 to 15 characters, can be composed of any printable character, but must not be made entirely of digits (0-9). The name is not case-sensitive. Default: no default	
IP	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 the IP is set to 0.0.0.0, then the router cannot initiate a virtual call to the remote end, but can still respond to a virtual call from the remote end of the tunnel. Default: no default	
TYpe	The type of L2TP call to add. Default: no default	
	ASYNc	The router acts as an LNS and the remote LAC activates an ACC call to connect to a remote user.
	ISDN	The router acts as an LNS and the remote LAC activates an ISDN call to connect to a remote user.
	VIrtual	An L2TP call is used to create a virtual link to a remote L2TP peer. There is no outgoing PSTN or ISDN call activated on the remote peer.
DIAL	The number called to connect to the remote location, from 1 to 63 decimal digits long. This must contain only the digits, including the access codes and area codes, required to dial from the remote L2TP server. The dial parameter is valid only when **type** is set to **isdn**. Default: no default	

Parameter (cont)	**Description** (cont)	
NUMber	How L2TP handles the sequence numbering of L2TP data packets. 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. Default: **off**	
	OFF	Sequence numbering is only used if the remote end requests sequencing.
	ON	Data packets are always numbered.
	STARTup	When the router is acting as an LNS, sequence numbering is only used during the initial PPP negotiation phase. After the initial PPP negotiation phase has concluded, sequence numbering of L2TP data packets ceases.
PASSword	The password used to authenticate the L2TP remote server before a tunnel is established. This must be between 1 to 31 characters long, is case-sensitive and can contain any printable character. Default: no default	
PRE13	Whether the call is compatible with pre-Internet Draft 13 L2TP implementations. Default: **off**	
	ON	The call is compatible.
	OFF	The call is not compatible.
PRECedence	The direction of precedence for the L2TP call in the event of a call collision. Call collisions occur when a call is activated at the same time as an incoming call selects the same call. The **precedence** parameter is only valid when **type** is set to **virtual**. Default: **in**	
	IN	The incoming call is accepted and the outgoing call is cleared.
	OUT	The outgoing call proceeds and the incoming call is cleared.
REMotecall	The name of an ACC, ISDN, or other call on the remote L2TP server. The type of call must match the value specified in 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 *name* must be between 1 to 15 characters, can be composed of any printable character, but must not be made entirely of digits (0-9). The name is not case-sensitive. If the **type** parameter is set to **virtual** and the **remotecall** parameter is not set, then the remote L2TP server creates a dynamic L2TP and dynamic PPP interface in response to a call initiated from this router. Default: no default	
SPeed	The maximum bandwidth of the connection, in bits per second. Default: **64000**	
SUBAddress	An ISDN subaddress, valid only when **type** is set to **isdn**. The *subaddress* must be 1 to 63 characters long, can contain any printable character, and is not case-sensitive. Default: no default	

Parameter (cont)	**Description** (cont)	
TOSreflect	Whether or not the TOS/DSCP field of a data packet within the L2TP tunnel should be reflected onto the encapsulated packet. This means that the tunnelled packet reflects the original packet's QoS information. Default: **off**	
	OFF, False, NO	The PPP frame's ToS byte is not copied to the outer IP header following L2TP encapsulation.
	ON, True, YES	The PPP frame's ToS byte is copied to the outer IP header following L2TP encapsulation.

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 that 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
```

To create a virtual call name "branch_office1" from a head office router to a branch office router at 192.168.45.1, where the branch office router has a similar L2TP call back to the head office named "head_office", use the command:

```
add l2tp call=branch_office1 rem=head_office ty=vi prec=out
   ip=192.168.45.1
```

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-ipadd} PPPTemplate=0..31
   [NUMber={OFF|ON|STARTup}] [PRE13={OFF|ON}]
   [PROXYAuth={OFF|ON}]
   [TOSreflect={OFF|ON|False|True|NO|YES}]
```

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 an LAC with a matching IP address, a dynamic PPP interface is created, and the associated PPP template is used to configure the PPP interface. The LNS mode must be enabled using the **enable l2tp server** command before these IP to PPP template mappings can be used.

Parameter	Description	
IP	The IP address or range of addresses for the remote L2TP LAC, in dotted decimal notation. When the router receives an L2TP frame from an LAC whose IP address matches the specified range, the router creates a dynamic PPP interface over the L2TP tunnel using the specified PPP template. Default: no default	
PPPTemplate	The identification number of the specific PPP template used when creating a dynamic PPP interface over the L2TP tunnel to the LAC. The specific template must already exist. See "Templates" on page 15-18 of Chapter 15, Point-to-Point Protocol (PPP) for more information about creating PPP templates. Default: no default	
NUMber	How L2TP handles the sequence numbering of L2TP data packets. 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. Default: **off**	
	OFF	Sequence numbering is only used if the remote end requests sequencing.
	ON	Data packets are always numbered.
	STARTup	When the router is acting as an LNS, sequence numbering is only used during the initial PPP negotiation phase. After the initial PPP negotiation phase has concluded, sequence numbering of L2TP data packets ceases.
PRE13	Whether the call is compatible with pre-Internet Draft 13 L2TP implementations. Default: **off**	
	OFF	The call is not compatible.
	ON	The call is compatible.

Parameter (cont)	**Description** (cont)	
PROXYAuth	Whether the router, acting as an LNS, performs Proxy Authentication of the PPP user if the LAC provides Authentication information. Default: **on**	
	OFF	The LNS does not perform Proxy Authentication.
	ON	The LNS performs Proxy Authentication.
TOSreflect	Whether or not the TOS/DSCP field of a data packet within the L2TP tunnel should be reflected onto the encapsulated packet. This means that the tunnelled packet reflects the original packet's QoS information. Default: **off**	
	OFF, False, NO	The PPP frame's ToS byte is not copied to the outer IP header following L2TP encapsulation.
	ON, True, YES	The PPP frame's ToS byte is copied to the outer IP header following L2TP encapsulation.

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-ipadd`*`}]`

Description This command sets the L2TP password used on the LNS for LAC connections originating from a specific IP address range. 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 20-19 overwrites the password added with the **set l2tp password** command on page 20-44.

Parameter	Description
PASSword	The authentication password used for the specific range of IP addresses. This can be between 1 to 31 characters long, and is case-sensitive. Valid characters are any printable character. Specify **none** if no password is required. Default: no default
IP	The IP address or range of addresses that the password applies to, in dotted decimal notation. Default: **0.0.0.0-255.255.255.255**

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
```

To specify the password “verysecret” for a single IP address within the previous example’s IP range, use the command:

```
add l2tp pass=verysecret ip=192.168.2.1
```

So, if the LAC IP address is 192.168.2.1 the password “verysecret” is used. If the LAC IP address is 192.168.2.2 the password “secret” is used.

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=1..65535]] [NUMber={OFF|ON}]
   [PASSword=password] [PRE13={ON|OFF}]
   [PREFix=prefix] [TIMEOut=8..300]
   [TOSreflect={OFF|ON|False|True|NO|YES}]
```

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.

Parameter	Description	
USER	The PPP username or type of PPP username this mapping matches to. This can be set to unstructured usernames, such as "bob", structured usernames, such as "bob@here.com" or domain names for users belonging to a particular domain, such as "here.com". Default: no default	
	mapping	A structured or unstructured username 1 to 63 characters long. Valid characters are any printable character and are not case-sensitive. To map all users with the username types "xxx@company.com", the mapping should be set to "company.com".
	ALL	The map entry matches any PPP sessions using any username.
	LOCAL	The map entry matches any PPP sessions using a username without any domain name information for authentication. For example "teleworker".
	NONE	The map entry matches PPP sessions for which no authentication is required.
	REMote	The map entry matches any PPP sessions using a username with domain name information for authentication. For example "john@maker.com".

Parameter (cont)	**Description** (cont)	
ACtion	The action taken when a PPP username matches the map entry. Default: no default	
	DATABase	The IP address and port information in the matching map entry is used to create an L2TP tunnel to the remote server. For this parameter to be valid, the IP address must be specified.
	DNSLookup	The user name information is used to perform a DNS lookup to determine the IP address of the remote L2TP server. If this succeeds then an L2TP tunnel is created to the remote server.
	IGNore	The authentication query from the dynamic PPP session, and the PPP session continues as a normal PPP link. No L2TP tunnel is created.
	RADius	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.
IP	The IP address of the remote L2TP server to call, in dotted decimal notation. Valid only when the **action** parameter is set to **database**. Default: no default	
POrt	The UDP port number to connect to on the remote L2TP server. The **port** parameter is used to optionally specify the port when **ip** is specified. Valid only when the **action** parameter is set to **database**. Default: no default	
NUMber	How L2TP handles the sequence numbering of L2TP data packets. 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. Default: **off**	
	OFF	Sequence numbering is only used if the remote end requests sequencing.
	ON	Data packets are always numbered.
	STARTup	When the router is acting as an LNS, sequence numbering is only used during the initial PPP negotiation phase. After the initial PPP negotiation phase has concluded, sequence numbering of L2TP data packets ceases.
PASSword	The password used to authenticate the L2TP remote server before a tunnel is established. This can be between 1 to 31 characters long, and is case-sensitive. Valid characters are any printable character. Default: no default	
PRE13	Whether the call is compatible with pre-Internet Draft 13 L2TP implementations. Default: **off**	
	OFF	The call is not compatible.
	ON	The call is compatible.

Parameter (cont)	**Description** (cont)	
PREFix	A string to prepend to the domain name portion of the username mapping string before performing a DNS lookup. The string can be from 1 to 31 characters long, of any printable character, and is not case sensitive. 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". This parameter is only valid when **action** is set to **dnslookup**. Default: no default	
TIMEOut	The maximum round trip time, in seconds, for L2TP traffic. Default: no default	
TOSreflect	Whether or not the TOS/DSCP field of a data packet within the L2TP tunnel should be reflected onto the encapsulated packet. This means that the tunnelled packet reflects the original packet's QoS information. Default: **off**	
	OFF, False, NO	The PPP frame's ToS byte is not copied to the outer IP header following L2TP encapsulation.
	ON, True, YES	The PPP frame's ToS byte is copied to the outer IP header following L2TP encapsulation.

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 us=maker.com ac=dnsl pref=l2tp
```

To add a record to tunnel all users having usernames without domain information, e.g. "john", to the remote L2TP server at 192.168.3.1:1701 (i.e. default L2TP port number), use the command:

```
add l2tp us=local ac=datab ip=192.168.3.1
```

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

deactivate l2tp call

Syntax `DEACTivate L2TP CALL={`*name*`|1..65535}`

Description This command deactivates an active 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 20-56.

Parameter	Description	
CALL	The *name* or *callid* of the L2TP call to deactivate. Default: no default	
	name	An L2TP call name 1 to 15 characters long that is not case-sensitive and can contain any printable character.
	1..65535	The call identification number of a dynamic call.

Examples To deactivate an 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*

Description This command deletes the specified predefined call to a remote L2TP server. The specified L2TP call must already exist. If the call is active, it is deactivated before it is deleted. The *name* specifies an L2TP call name 1 to 15 characters long that is not case-sensitive and can contain any printable character.

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-ipadd`*`}`

Description This command deletes the association between a PPP template and incoming L2TP calls from an IP address or IP address range. The router uses this association when it is acting as an LNS.

The association is identified by specifying the IP address or IP address range, in dotted decimal notation, that was originally specified by the **add l2tp ip** command on page 20-22. Once you remove the association between an IP address range and a PPP template, incoming calls from that IP range will create a dynamic PPP interface using the default PPP template instead of a specific template, unless their IP address falls within the address range specified with another **add l2tp ip** entry.

Examples To stop L2TP calls from the LAC with the IP address 192.168.74.2 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-ipadd`*`|ALL}]`

Description This command removes the L2TP password used on an LNS for LAC connections originating from a specific IP address range. This command affects passwords set using the **add l2tp password** command. It does not affect the global password set using the **set l2tp password** command, unless you have saved the router configuration using the **create config** command. The **create config** command changes the **set l2tp password** command into an **add l2tp password** command.

Parameter	Description	
IP	The range or IP addresses, in dotted decimal notation, to remove a password on. The specific range must match an existing password range. Note that if there are two address ranges each with a password assigned, and one address range is a subset of the other, then deleting the wider address range will not delete the password assigned to the smaller subset range. Default: **0.0.0.0-255.255.255.255**	
	ipadd	The IP address range selected for password deletion.
	ipadd-ipadd	The IP address range selected for password deletion.
	ALL	Removes all passwords from all configured address ranges.

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}`

Description This command deletes a mapping between a username provided for PPP authentication and the action L2TP takes on matching that username. To see the user mapping entries on the router, use the **show l2tp user** command.

Parameter	Description	
USer	The specific PPP username, or type of PPP username, the mapping entry is deleted for. Default: no default	
	mapping	The mapping for the specified user is deleted. This can be a structured or unstructured username 1 to 63 characters long. Valid characters are any printable character and are not case-sensitive.
	ALL	The mapping for **all** is deleted. When set, this parameter matches any PPP sessions using any username.
	LOCAL	The mapping for **local** is deleted. When set, this parameter matches any PPP sessions using a username without any domain name information for authentication. For example "teleworker".
	NONE	The mapping for **none** is deleted. When set, this parameter matches PPP sessions for which no authentication is required.
	REMote	The mapping for **remote** is deleted. When set, this parameter matches any PPP sessions using a username with domain name information for authentication. For example "john@maker.com".

Examples To delete a record used to map all users with usernames of the type "xxx@maker.com" (refer to the **add l2tp user** command example), use the command:

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

To delete the record used to map all usernames without domain information, for example "john", use the command:

```
del l2tp us=local
```

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|DECode|PKT|STAte}
   [CALL[=1..65535]|TUNnel[=1..65535]]
```

Description

This command disables debugging of the specified tunnel or call. If both **call** and **tunnel** are omitted from the command, debugging is disabled on all currently active calls and tunnels, and all calls and tunnels created from that time, until debugging is enabled.

Parameter	Description	
DEBug	The debugging options to disable on the specified call or tunnel, or on all calls and tunnels. Default: no default	
	ALL	All debugging is disabled.
	DECode	Decode debugging is disabled. When enabled, this decodes control messages and payload message headers into a human-readable format.
	PKT	Packet debugging is disabled. When enabled, this displays hexadecimal data for all control and payload packets.
	STAte	State debugging is disabled. When enabled, this displays the state transitions.
CALL	Whether debugging is disabled for an L2TP call. If no identification number is specified debugging is disabled for all currently active calls and all calls created from that time, until call debugging is enabled. Default: no default	
	1..65535	The identification number of a specific dynamic L2TP call.
TUNnel	The tunnel for which debugging is disabled. If no identification number is specified, debugging is disabled for all currently active tunnels and all tunnels created from that time, until call debugging is enabled. Default: no default	
	1..65535	The identification number of a specific L2TP tunnel.

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={BOTH|LAC|LNS}`

Description This command selectively disables the server modes of the L2TP process. By default, both LNS and LAC server modes are disabled.

Parameter	Description	
SERVER	The L2TP server mode to disable. Default: no default	
	BOTH	Both the LAC and LNS server modes are disabled.
	LAC	LAC server mode is disabled. The router no longer intercepts ACC calls, ISDN calls, or PPPoE sessions and redirects them over L2TP tunnels to remote LNS servers.
	LNS	LNS server mode is disabled. The router no longer acts as a termination point for L2TP tunnels and calls.

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 L2TP on the router, so that incoming ACC calls, ISDN calls, L2TP calls or PPPoE sessions activate the associated L2TP call. L2TP is disabled 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|DECode|PKT|STAte}
   [CALL[=1..65535]|TUNnel[=1..65535]] [TIMEOut=1..300]
```

Description

This command enables debugging of the specified tunnel or call. If both **call** and **tunnel** are omitted from the command, debugging is enabled on all currently active calls and tunnels, and all calls and tunnels created from that time, until debugging is disabled.

Parameter	Description	
DEBug	The debugging options to enable on the specified call or tunnel, or on all currently active calls and tunnels. Default: no default	
	ALL	All debugging is enabled.
	DECode	Decode debugging is enabled (Figure 20-5 on page 20-36, Table 20-1 on page 20-36). This decodes control and payload messages into a human-readable format. For control packets, all of the message is decoded. For payload packets, only the header is decoded. The first 64 bytes of the encapsulated frame is also displayed, but remains in hexadecimal format.
	PKT	Packet debugging is enabled (Figure 20-6 on page 20-37, Table 20-2 on page 20-37). This displays hexadecimal data for all control and payload packets.
	STAte	State debugging is enabled (Figure 20-7 on page 20-37, Table 20-3 on page 20-38). This displays the state transitions.
CALL	Whether debugging is enabled for an L2TP call. If no identification number is specified debugging is enabled for all currently active calls and all calls created from that time, until call debugging is disabled. Default: no default	
	1..65535	The identification number of a specific dynamic L2TP call.
TUNnel	The tunnel for which debugging is enabled. If no identification number is specified, debugging is enabled for all currently active tunnels and all tunnels created from that time, until call debugging is disabled. Default: no default	
	1..65535	The identification number of a specific L2TP tunnel.
TIMEOut	The length of time, in seconds, that the router produces debug information before all debugging modes are automatically disabled. Default: no time limit set (debugging continues until turned off using the **disable l2tp debug** command)	

Figure 20-5: Example output from the **enable l2tp debug=decode** command

```
18:07:20 L2TP DECODE: Rx [TID:0 CID:0 from 192.168.1.1:1701]
  Header:
    Version: 2  Type: Control  Flags: T,L,S  Length: 107
    Tunnel ID: 0  Session ID: 0
    Sequence Numbers: Ns 0  Nr 0
  Attribute Value Pairs (AVPs):
    Message Type (0)
      Flags: M     Len: 8     Value: SCCRQ
    Protocol Version (2)
      Flags: M     Len: 8     Value: 1.0
    Host Name (7)
      Flags: M     Len: 12    Value: L2TP A
    Framing Capabilities (3)
      Flags: M     Len: 10    Value: Async Sync
    Assigned Tunnel ID (9)
      Flags: M     Len: 8     Value: 36082
    Bearer Capabilities (4)
      Flags: M     Len: 10    Value: Analog Digital
    Tie Breaker (5)
      Flags: -     Len: 14
      Value: 761cbc695895ce13
    Firmware Revision (6)
      Flags: -     Len: 8     Value: 0207
    Vendor Name (8)
      Flags: -     Len: 9     Value: ATI
    Receive Window Size (10)
      Flags: M     Len: 8     Value: 4

18:07:20 L2TP DECODE: Tx [TID:1618 CID:3612 to 192.168.1.1:1701]
  Header:
    Version: 2  Type: Payload  Flags: L,P  Length: 34
    Tunnel ID: 36082  Session ID: 21368
  Payload:
    ff03c021 01040016 01040678 0408c025 00001770 05061537 023c
```

Table 20-1: Parameters in the output of the **enable l2tp debug=decode** command

Parameter	Meaning
timestamp	The system time when the entry was added.
L2TP DECODE	Indicates that the output is L2TP decode debugging.
Tx	Indicates that the router transmitted the packet to a peer.
Rx	Indicates that the router received the packet from a peer.
TID	The local tunnel ID number associated with the packet.
CID	The local call ID number associated with the packet. The first packet received from a peer will state the IP range and port number of the call instead of a call ID number.
Header	Header information for the packet. This specifies the version, type, flags, length, tunnel ID, session ID, sequence numbers and any padding. For detailed information about these, see RFC 2661.
Attribute Value Pairs (AVPs)	A list of the AVPs in the packet. For detailed information about individual AVPs, see RFC 2661.
Payload	The first 64 bytes of the encapsulated frame from a payload packet. This displays as raw data in hexadecimal format.

Figure 20-6: Example output from the **enable l2tp debug=pkt** command

```
18:31:57 L2TP PKT: Tx [TID:36082 CID:0 to 192.168.1.2:1701]
c802006b 00000000 00000000 80080000 00000001 80080000 00020100 800c0000
00074c32 54502041 800a0000 00030000 00038008 00000009 8cf2800a 00000004
00000003 000e0000 0005761c bc695895 ce130008 00000006 02070009 00000008
41544980 08000000 0a0004

18:31:57 L2TP PKT: Rx [TID:36082 CID:0 from 192.168.1.2:1701]
c802005d 8cf20000 00000001 80080000 00000002 80080000 00020100 800a0000
00030000 0003800c 00000007 4c325450 20428008 00000009 2d62800a 00000004
00000003 00080000 00060207 00090000 00084154 49800800 00000a00 04

18:31:57 L2TP PKT: Tx [TID:36082 CID:0 to 192.168.1.2:1701]
c8020014 2d620000 00010001 80080000 00000003

18:31:57 L2TP PKT: Tx [TID:36082 CID:21368 to 192.168.1.2:1701]
41020022 2d628d06 ff03c021 01040016 01040678 0408c025 00001770 0506530c
6ed4
```

Table 20-2: Parameters in the output of the **enable l2tp debug=pkt** command

Parameter	Meaning
timestamp	The system time when the entry was added.
L2TP PKT	Indicates that output is L2TP packet debugging.
Tx	Indicates that the router transmitted the packet to a peer.
Rx	Indicates that the router received the packet from a peer.
TID	The local tunnel ID number associated with the packet.
CID	The local call ID number associated with the packet.
hexadecimal number	The packet data in hexadecimal format. For more information see RFC 2661.

Figure 20-7: Example output from the **enable l2tp debug=state** command

```
18:31:57 L2TP STATE: Tunnel State Change
  TID:36082 to 192.168.1.2:1701
          idle --> wait-ctl-reply
18:31:57 L2TP STATE: Tunnel State Change
  TID:36082 to 192.168.1.2:1701
          wait-ctl-reply --> established

18:31:57 L2TP STATE: Call State Change
  TID:36082 CID:21368 to 192.168.1.2:1701
          idle --> wait-reply
18:31:57 L2TP STATE: Call State Change
  TID:36082 CID:21368 to 192.168.1.2:1701
          wait-reply --> established
```

Table 20-3: Parameters in the output of the **enable l2tp debug=state** command

Parameter	Meaning
timestamp	The system time when the entry was added.
L2TP STATE	Indicates that output is L2TP state debugging.
Call State Change	Indicates that a call changed its state.
Tunnel State Change	Indicates that a tunnel changed its state.
TID	The local tunnel ID number associated with the state change.
CID	The local call ID number associated with the state change. The first packet received from a peer will state the IP range and port number of the call instead of a call ID number.
to *ipadd*	The IP address associated with the state change.
state - -> state	The original state followed by the current state. For detailed information about the types of state changes, see RFC 2661.

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

```
ena 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. By default, both LNS and LAC server modes are disabled.

Parameter	Description	
SERVER	The L2TP server mode to enable. Default: no default	
	BOTH	Both the LAC and LNS server modes are enabled.
	LAC	LAC server mode is enabled. The router intercepts ACC calls, ISDN calls, or PPPoE sessions and redirects them over L2TP tunnels to remote LNS servers.
	LNS	LNS server mode is enabled. The router acts as a termination point for L2TP tunnels and calls.

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

reset l2tp counter

Syntax `RESET L2TP COUnter`

Description This command resets the general L2TP counters, which are displayed using the **show l2tp counter** command.

Example To reset the L2TP counters, use the command:

```
reset l2tp cou
```

See Also **show l2tp counter**

set l2tp call

Syntax

```
SET L2TP CALL=name [DIAL=number] [IP=ipadd]
   [NUMber={OFF|ON|STARTup}] [PASSword=password]
   [PRE13={OFF|ON}] [PRECedence={IN|OUT}]
   [REMotecall=name] [SPeed=300..4294967295]
   [SUBAddress=subaddress]
   [TOSreflect={OFF|ON|False|True|NO|YES}]
   [TYpe={ASYNc|ISDN|VIrtual}]
```

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.

Parameter	Description	
CALL	The name of the L2TP call to set. An L2TP call with the same name must already exist. The *name* must be between 1 to 15 characters, can be composed of any printable character, but must not be made entirely of digits (0-9). The name is not case-sensitive. Default: no default	
DIAL	The number called to connect to the remote location, from 1 to 63 decimal digits long. This must contain only the digits, including the access codes and area codes, required to dial from the remote L2TP server. The dial parameter is valid only when **type** is set to **isdn**. Default: no default	
IP	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 the IP is set to 0.0.0.0, then the router cannot initiate a virtual call to the remote end, but can still respond to a virtual call from the remote end of the tunnel. Default: no default	
NUMber	How L2TP handles the sequence numbering of L2TP data packets. 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. Default: **off**	
	OFF	Sequence numbering is only used if the remote end requests sequencing.
	ON	Data packets are always numbered.
	STARTup	When the router is acting as an LNS, sequence numbering is only used during the initial PPP negotiation phase. After the initial PPP negotiation phase has concluded, sequence numbering of L2TP data packets ceases.
PASSword	The password used to authenticate the L2TP remote server before a tunnel is established. This must be between 1 to 31 characters long, is case-sensitive and can contain any printable character. Default: no default	

Parameter (cont)	**Description** (cont)	
PRE13	Whether the call is compatible with pre-Internet Draft 13 L2TP implementations. Default: **off**	
	OFF	The call is not compatible.
	ON	The call is compatible.
PRECedence	The direction of precedence for the L2TP call in the event of a call collision. Call collisions occur when a call is activated at the same time as an incoming call selects the same call. The **precedence** parameter is only valid when **type** is set to **virtual**. Default: **in**	
	IN	The incoming call is accepted and the outgoing call is cleared.
	OUT	The outgoing call proceeds and the incoming call is cleared.
REMotecall	The name of an ACC, ISDN, or other call on the remote L2TP server. The type of call must match the value specified in 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 *name* must be between 1 to 15 characters, can be composed of any printable character, but must not be made entirely of digits (0-9). The name is not case-sensitive. If the **type** parameter is set to **virtual** and the **remotecall** parameter is not set, then the remote L2TP server creates a dynamic L2TP and dynamic PPP interface in response to a call initiated from this router. Default: no default	
SPeed	The maximum bandwidth of the connection, in bits per second. Default: **64000**	
SUBAddress	An ISDN subaddress, valid only when **type** is set to **isdn**. The *subaddress* must be 1 to 63 characters long, can contain any printable character, and is not case-sensitive. Default: no default	
TOSreflect	Whether or not the TOS/DSCP field of a data packet within the L2TP tunnel should be reflected onto the encapsulated packet. This means that the tunnelled packet reflects the original packet's QoS information. Default: **off**	
	OFF, False, NO	The PPP frame's ToS byte is not copied to the outer IP header following L2TP encapsulation.
	ON, True, YES	The PPP frame's ToS byte is copied to the outer IP header following L2TP encapsulation.
TYpe	The type of L2TP call that is set. Default: no default	
	ASYNc	The router acts as an LNS and the remote LAC activates an ACC call to connect to a remote user.
	ISDN	The router acts as an LNS and the remote LAC activates an ISDN call to connect to a remote user.
	VIrtual	An L2TP call is used to create a virtual link to a remote L2TP peer. There is no outgoing PSTN or ISDN call activated on the remote peer.

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={OFF|ON}`

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. The default is **on**.

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={0..299|NONE}`

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

Parameter	Description	
FILter	Specifies either an IP filter or **none**. IP filters are created using the **add ip filter** command on page 22-70 of Chapter 22, Internet Protocol (IP). Default: no default	
	0..299	The identification number of an existing IP filter. The router is only able to communicate with remote L2TP servers that are included by the IP filter. This must match some combination of source address, destination address, protocol and/or port number.
	NONE	Filtering is disabled and there are no restrictions on the remote L2TP servers with which the router can communicate.

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}`

Description This command is superseded by the **add l2tp password** command. The router converts the **set l2tp password** command into an **add l2tp password** command when you save the router configuration using the **create config** command.

This command sets a global password on the LNS when authenticating tunnel creation with all other L2TP servers. The **delete l2tp password** command does not work for a password set using this command, unless you have saved the router configuration as described above. To delete a password set using this command, specify the option **none**.

Parameter	Description	
PASSword	The global password used. Default: no default	
	password	A global password is created. This must be between 1 to 31 characters long, can contain any printable character and is case-sensitive.
	NONE	No global password is set. Any previously set global password is removed.

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

```
set l2tp pass=secret
```

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

set l2tp user

Syntax

```
SET L2TP USer={mapping|ALL|LOCAL|NONE|REMote}
   [ACtion={DATABase|DNSLookup|IGNore|RADius}]
   [IP=ipadd [POrt=1..65535]] [NUMber={OFF|ON}]
   [PASSword=password] [PRE13={OFF|ON}]
   [PREFix=prefix] [TIMEOut=8..300]
   [TOSreflect={OFF|ON|False|True|NO|YES}]
```

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.

Parameter	Description	
USer	The PPP username or type of PPP username this mapping matches to. This can be set to unstructured usernames, such as "bob", structured usernames, such as "bob@here.com" or domain names for users belonging to a particular domain, such as "here.com". Default: no default	
	mapping	A structured or unstructured username 1 to 63 characters long. Valid characters are any printable character and are not case-sensitive. To map all users with the username types "xxx@company.com", the mapping should be set to "company.com".
	ALL	The map entry matches any PPP sessions using any username.
	LOCAL	The map entry matches any PPP sessions using a username without any domain name information for authentication. For example "teleworker".
	NONE	The map entry matches PPP sessions for which no authentication is required.
	REMote	The map entry matches any PPP sessions using a username with domain name information for authentication. For example "john@maker.com".

Parameter (cont)	**Description** (cont)	
ACtion	The action taken when a PPP username matches the map entry. Default: no default	
	DATABase	The IP address and port information in the matching map entry is used to create an L2TP tunnel to the remote server. For this parameter to be valid, the IP address must be specified.
	DNSLookup	The user name information is used to perform a DNS lookup to determine the IP address of the remote L2TP server. If this succeeds then an L2TP tunnel is created to the remote server.
	IGNore	The authentication query from the dynamic PPP session, and the PPP session continues as a normal PPP link. No L2TP tunnel is created.
	RADius	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.
IP	The IP address of the remote L2TP server to call, in dotted decimal notiation. Valid only when **action** is set to **database**. Default: no default	
POrt	The UDP port number to connect to on the remote L2TP server. The **port** parameter is used to optionally specify the port when **ip** is specified. Valid only when **action** is set to **database**. Default: no default	
NUMber	How L2TP handles the sequence numbering of L2TP data packets. 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. Default: **off**	
	OFF	Sequence numbering is only used if the remote end requests sequencing.
	ON	Data packets are always numbered.
	STARTup	When the router is acting as an LNS, sequence numbering is only used during the initial PPP negotiation phase. After the initial PPP negotiation phase has concluded, sequence numbering of L2TP data packets ceases.
PASSword	The password used to authenticate the L2TP remote server before a tunnel is established. This can be between 1 to 31 characters long, and is case-sensitive. Valid characters are any printable character. Default: no default	
PRE13	Whether the call is compatible with pre-Internet Draft 13 L2TP implementations. Default: **off**	
	OFF	The call is not compatible.
	ON	The call is compatible.

Parameter (cont)	**Description** (cont)	
PREFix	A string to prepend to the domain name portion of the username mapping string before performing a DNS lookup. The string can be from 1 to 31 characters long, of any printable character, and is not case sensitive. 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". This parameter is only valid when **action** is set to **dnslookup**. Default: no default	
TIMEOut	The maximum round trip time, in seconds, for L2TP traffic. Default: no default	
TOSreflect	Whether or not the TOS/DSCP field of a data packet within the L2TP tunnel should be reflected onto the encapsulated packet. This means that the tunnelled packet reflects the original packet's QoS information. Default: **off**	
	OFF, False, NO	The PPP frame's ToS byte is not copied to the outer IP header following L2TP encapsulation.
	ON, True, YES	The PPP frame's ToS byte is copied to the outer IP header following L2TP encapsulation.

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`

Description This command displays the global configuration and status of L2TP (Figure 20-8, Table 20-4).

Figure 20-8: 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 20-4: Parameters in 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 times the router has received L2TP packets containing errors.
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 server
enable l2tp
enable l2tp server
set l2tp checksum
set l2tp filter
set l2tp password
show l2tp counter

show l2tp call

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

Description This command displays information about the specified call definition or all defined calls (Figure 20-9, Table 20-5). A call *name* is between 1 to 15 characters, can be composed of any printable character, but cannot be made entirely of digits (0-9). The name is not case-sensitive.

Figure 20-9: 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
  ToS Reflect .............. off
```

Table 20-5: Parameters in 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 an 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.

Table 20-5: Parameters in output of the **show l2tp call** command (cont)

Parameter	Meaning
Subaddress	The ISDN subaddress to use when the Type field is set to "isdn", or "not set".
ToS Reflect	Whether the TOS/DSCP field of data packets within the L2TP tunnel is reflected onto the encapsulated packet.

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 counter

Syntax `SHow L2TP COUnter`

Description The **counter** parameter displays the global configuration and status of L2TP and general counters for L2TP (Figure 20-10, Table 20-6 on page 20-53).

Figure 20-10: 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 20-6: Parameters in 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 20-6: Parameters in output of the **show l2tp counter** command (cont)

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 counters for L2TP, use the command:

```
sh l2tp coun
```

See Also **reset l2tp counter**
set l2tp checksum
set l2tp filter
show l2tp

show l2tp ip

Syntax `SHow L2TP IP`

Description This command displays the associations between PPP templates and remote L2TP peers (Figure 20-11, Table 20-7).

Figure 20-11: 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
  ToS Reflect .................. off
  Proxy Authentication ......... on
-------------------------------------------------------------
```

Table 20-7: Parameters in 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; one of "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.
ToS Reflect	Whether the TOS/DSCP field of data packets within the L2TP tunnel is reflected onto the encapsulated packet.
Proxy Authentication	Whether the router, acting as an LNS, performs Proxy Authentication of the PPP user if the LAC provides Authentication information; one of "on" or "off".

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[=1..65535]`

Description This command displays information about active L2TP tunnels.

Parameter	Description	
TUNnel	Whether detailed information about a specific tunnel or all tunnels is displayed. A summary of the relevant active calls is displayed with each tunnel (Figure 20-12, Table 20-8 on page 20-57). Default: no default	
	not specified	Detailed information about each active tunnel is displayed, including a summary of the calls associated with each tunnels.
	1..65535	Detailed information about the specified tunnel is displayed, including the calls associated with the tunnel.

Figure 20-12: 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
  Local IP Address ............ 172.20.15.254
  Local UDP Port .............. 1701
  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
    Tunnel 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 20-8: Parameters in 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 "disabled" or enabled on the tunnel. If enabled, the type of debugging is displayed; one of "state", "packet" or "decode".
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.
Local IP Address	The IP address that was used to establish the tunnel
Local UDP Port	The port that the communication was received on
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 version) 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 4-31 of Chapter 4, Configuring and Monitoring the System.
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.

Table 20-8: Parameters in output of the **show l2tp tunnel** command (cont)

Parameter	Meaning
Tunnel ID	Tunnel identification number of the tunnel associated with this 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.
State	The status of the call, one of "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.

Example To show all tunnels, use the command:

```
sh l2tp tun=3
```

See Also
activate l2tp call
add l2tp call
add l2tp password
deactivate l2tp call
delete l2tp call
delete l2tp user
disable l2tp debug
enable l2tp debug
set l2tp call
set l2tp user
show l2tp
show l2tp call

show l2tp tunnel call

Syntax `SHow L2TP TUNnel CALL[=1..65535]`

Description This command displays information about active L2TP calls.

Parameter	Description	
CALL	Detailed or summary information is shown for calls. Default: no default	
	not specified	Summary information is displayed for every L2TP call on the router. (Figure 20-13, Table 20-9).
	1..65535	Counters for the specified call are displayed (Figure 20-14 on page 20-60, Table 20-10 on page 20-60).

Figure 20-13: Example output of summary information from the **show l2tp tunnel call** command

```
Call ID ......................... 35267
Tunnel ID ....................... 24751
Server Type ..................... LAC
Started ......................... 12-Apr-2006 11:04:50
Username ........................ not set
State ........................... established
Call Serial Number .............. 3
Remote Call ID .................. 10833

Call ID ......................... 45371
Tunnel ID ....................... 24751
Server Type ..................... LAC
Started ......................... 12-Apr-1998 10:52:38
Username ........................ not set
State ........................... established
Call Serial Number .............. 1
Remote Call ID .................. 60415
```

Table 20-9: Parameters in output of the **show l2tp tunnel call** command

Parameter	Meaning
Call ID	Call identification number for an active call.
Tunnel ID	Tunnel identification number of the tunnel associated with this 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.
State	The status of the call, one of “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 20-9: Parameters in output of the **show l2tp tunnel call** command (cont)

Parameter	Meaning
Remote Call ID	Call identification number for this call on the remote L2TP server.

Figure 20-14: Example output from the **show l2tp tunnel call** command for a specific call

```
Call ID ..................... 52221
Tunnel ID ................... 19223
Server Type ................. LAC
Started ..................... 01-Apr-2006 16:45:51
Username .................... not set
Sequence Numbers ............ off
Debug ....................... packet
Debug Device ................ 16
Call Serial Number .......... 2
Remote Call ID .............. 54079
Authentication type ......... 4
Physical Channel ............ 0
Framing ..................... sync
Bearer ...................... none
Connect Speed ............... 0
Calling number .............. not set
Private Group ID ............ not set
In Discards ................. 0
In Packets .................. 58
In Bytes .................... 916
Out Packets ................. 58
Out Bytes ................... 916
```

Table 20-10: Parameters in output of the **show l2tp tunnel call** command for a specific call

Parameter	Meaning
Call ID	Call identification number assigned to the active call.
Tunnel ID	Tunnel identification number assigned to the active tunnel.
Server Type	The server mode for this call; one of "LAC" or "LNS".
Started	Date and time the call was initiated.
Username	Username associated with this call.
State	The status of call; one of "idle", "wait-cs-answer", "wait-connect", or "established".
Sequence Numbers	Whether payload packet sequence numbering is active. One of "off", "on", "startup" or "LNS set to on".
Debug	Whether debugging is "disabled" or enabled on the tunnel. If enabled, the type of debugging is displayed; one of "state", "packet" or "decode".
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.

Table 20-10: Parameters in output of the **show l2tp tunnel call** command for a specific call (cont)

Parameter	Meaning
Physical Channel	Remote physical channel number used for the call. The meaning is vendor-specific.
Framing	Framing used by the remote L2TP server for the connection to the final destination' one of "none", "sync", "async", or "sync+async".
Bearer	Bearer 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.
Calling Number	Calling number of 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.
Called Number	Number dialed 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. This only displays when the router is acting as an LNS.
Sub-Address	ISDN subaddress used when the Dialed Number field contains an ISDN number, or "not set". This only displays when the router is acting as an LNS.
Private Group ID	Number used to associate the call with a particular customer group.
Next Sent	The send number used in the next L2TP payload packet transmitted for this call. This displays only when numbering payload packets.
Next Received	The receive number expected in the next L2TP payload packet received for this call. This displays only when numbering payload packets.
In Discards	Number of incoming L2TP payload packets 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.
Parameters only displayed when the call originates from a remote L2TP server	
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 use for the call. The meaning is vendor-specific.
Remote Framing	Framing requested by the remote L2TP server to use for the local connection to the final destination; either "none", "digital", "analog", or "digital+analog".
Remote Bearer	Bearer requested by the remote L2TP server to use for the local connection to the final destination; either "none", "digital", "analog", or "digital+analog".

Table 20-10: Parameters in output of the **show l2tp tunnel call** command for a specific call (cont)

Parameter	Meaning
Remote Connect Speed	Speed requested by the remote L2TP server for the local connection.
Remote Calling 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.
Remote Called Number	Number passed on 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. This displays only when the router is acting as an LAC.
Remote Sub-Address	ISDN subaddress passed on by the remote L2TP server to use when the Dialed Number field contains an ISDN number, or "not set". This displays only when the router is acting as an LAC.
Remote Private Group ID	Number passed by the remote L2TP server to associate the call with a particular customer group.

To show a summary of all calls active on the router, use the command:

```
sh l2tp tun call
```

To show details about the call with ID 2785, use the command:

```
sh l2tp tun call=2785
```

See Also

activate l2tp call
add l2tp call
add l2tp password
deactivate l2tp call
delete l2tp call
delete l2tp user
disable l2tp debug
enable l2tp debug
set l2tp call
set l2tp user
show l2tp
show l2tp call

show l2tp tunnel call counter

Syntax `SHow L2TP TUNnel CALL[=1..65535] COUnter`

Description This command displays detailed counters for active L2TP calls.

Parameter	Description	
CALL	Detailed counters for L2TP calls are displayed (Figure 20-15, Table 20-11). Default: no default	
	not specified	Counters for every L2TP call on the router are displayed.
	1..65535	Counters for the specified call are displayed.

Figure 20-15: Example output from the **show l2tp tunnel call counter** command

```
Call ID ......................... 32760
Tunnel ID ....................... 19968
Server Type ..................... LAC
Started ......................... 11-Apr-2006 11:29:37
Username ........................ not set
State ........................... established
Call Serial Number .............. 3
Remote Call ID .................. 10833
In Packets ...................... 9
In Bytes ........................ 264
In Payload Packets .............. 9
In Payload Packets With Data .... 9
In Payload Packets No Data ...... 0
Processed Payload Packets ....... 9
In Order Payload Packets ........ 0
Out Of Order Payload Packets .... 0
Order Discarded Packets ......... 0
In Discards ..................... 0
Out Packets ..................... 9
Out Bytes ....................... 264
Out Payload Packets ............. 9
Out Payload Packets With Data ... 9
Out Payload Packets No Data ..... 0
Out Flow Payload Timeouts ....... 0
```

Table 20-11: Parameters in 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.

Table 20-11: Parameters in output of the **show l2tp tunnel call counter** command

Parameter	Meaning
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.
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 counters for the call ID 36, use the command:

```
sh l2tp tun 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 tunnel counter

Syntax `SHow L2TP TUNnel[=1..65535] COUnter`

Description This command displays detailed counters for L2TP tunnels.

Parameter	Description	
TUNnel	Detailed counters for L2TP tunnels are displayed (Figure 20-16, Table 20-12). Default: no default	
	not specified	Counters for every L2TP tunnel on the router are displayed.
	1..65535	Counters for the specified tunnel are displayed.

Figure 20-16: Example output from the **show l2tp tunnel counter** command

```
Tunnel ID ..................... 12
  State ....................... established
  Started ..................... 21-Apr-2006 14:13:39
  Local IP Address ............ 192.168.1.1
  Local UDP Port .............. 1701
  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 .... 3
  In Control Packets No Data ...... 2
  Processed Control Packets ....... 5
  In Order Control Packets ........ 5
  Out Of Order Control Packets .... 0
  Order Discarded Ctl Packets ..... 0
  Out Control Packets ............. 6
  Out Control Packets With Data ... 6
  Out Control Packets No Data ..... 0
  Out Flow Control Timeouts ....... 0
```

Table 20-12: 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.
Local IP address	IP address used by the tunnel at this end.
Local UDP Port	UDP port used by the tunnel at this end.
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.

Table 20-12: Parameters in the output of the **show l2tp tunnel counter** command (cont)

Parameter	Meaning
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 4-31 of Chapter 4, Configuring and Monitoring the System.
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.
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.

Examples

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

```
sh l2tp tun 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`*`]`

Description This command displays the user mapping entries, as originally defined in the **add l2tp user** and **set l2tp user** commands.

Parameter	Description	
USer	Selects the user mapping entries to display (Figure 20-17, Table 20-13). Default: all users shown	
	none specified	All user mapping entries are shown.
	mapping	A structured or unstructured username 1 to 63 characters long. Valid characters are any printable character and are not case-sensitive. Only the specified user mapping displays. The mapping ranges "all", "local", "none" and "remote" can be displayed individually using this command.

Figure 20-17: 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
  ToS Reflect .............. off

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

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

Table 20-13: Parameters in 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; one of "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**.
ToS Reflect	Whether the TOS/DSCP field of data packets within the L2TP tunnel is reflected onto the encapsulated packet.
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