

Configuring L2F

5

This chapter describes Layer Two Forwarding (L2F), which is a Cisco Systems proprietary protocol.

Topic	Page
Overview	5-1
References	5-4
Functionality	5-5
Configuring L2F	5-9
Managing L2F	5-15
Monitoring L2F	5-17

Overview

Layer Two Forwarding (L2F) provides a method for virtual dial-up service over the Internet. The traditional method for a remote user to access a company's network is through remote access equipment that is directly attached to the corporate network. This method requires a significant investment in equipment and support in addition to the cost of telephone charges for remote workers calling in to the access equipment.

By employing L2F, an Internet service provider (ISP) can provide local access for the remote worker and forward their data traffic through a tunnel to the corporate network. This method allows a company to outsource the investment in remote access equipment to the ISP, while retaining full control over access to the corporate network. In particular, L2F allows leveraging multiple protocols and private addressing across the existing Internet infrastructure.

Terms

Table 5-1 defines terms and abbreviations that are used in this discussion of L2F.

Table 5-1 L2F Terms and abbreviations

Term	Definition
Call	A session or connection request between a home gateway and an NAS.
Client	A remote end-user system. Sometimes referred to as client PC.
Connection	The extended PPP session across an L2F Tunnel. An L2F connection is equivalent to an L2TP session.
Home gateway	A node that acts as the server side of an L2F tunnel endpoint and is a peer to the NAS. The logical termination point of a PPP connection that is being tunneled from the remote system by the LAC. A home gateway is equivalent to an LNS in L2TP applications. You cannot configure the ERX system as a home gateway.
Incoming call	A connection request initiated by a network access server. (Note that L2F does not support outgoing calls.)
L2F	Layer Two Forwarding protocol. Cisco-proprietary protocol that tunnels link-layer frames (PPP or SLIP) over networks.
L2TP	Layer Two Tunneling Protocol. The IETF open protocol that tunnels PPP over networks.
LAC	L2TP access concentrator. The client side of an L2TP tunnel. The LAC is equivalent to an NAS in L2F applications.
LNS	L2TP network server. The server side of L2TP. The LNS is equivalent to a home gateway in L2F applications.
NAS	Network access server. A node that acts as the client side of an L2F tunnel endpoint and is a peer to the home gateway. An NAS sits between a home gateway and a remote system and forwards packets to and from each. The NAS is equivalent to a LAC in L2TP applications. The ERX system acts as the NAS.
Proxy authentication	Initial PPP authentication performed on behalf of the home gateway by the NAS. On the ERX system this will inform the system if this PPP session is to be tunneled or terminated.
Proxy LCP	Initial LCP negotiation performed by the NAS on behalf of the home gateway.
Tunnel	The control connection between the NAS and the home gateway. A tunnel is an aggregation of one or more connections.

Implementing L2F

L2F encapsulates layer 2 packets, in this case PPP packets, for transmission across a network. L2F uses the following components:

- NAS – forwards traffic to and from the remote client and the home gateway. The ERX system acts as the NAS.
- Home gateway – A peer to the NAS.
- Tunnel – A direct path between the NAS and the home gateway. A tunnel contains several connections.
- Connection – A PPP connection in a tunnel. In the CLI, an L2F connection is referred to as a session.
- Destination – The remote end of the tunnel. In this case, the home gateway is the destination.

As shown in Figure 5-1, the ERX system, configured as an NAS, receives packets from a remote client and forwards them through a tunnel to a home gateway on a remote network.

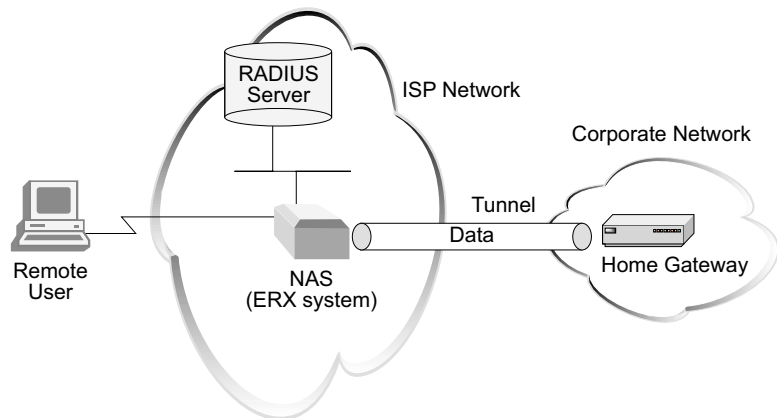


Figure 5-1 Typical L2F setup

The ERX system creates tunnels dynamically by using AAA authentication parameters and transmits L2F packets to the home gateway via UDP/IP. Traffic travels in L2F connections. A tunnel is an aggregation of one or more connections.

How L2F Works

The ERX system, acting as the NAS, creates destinations, tunnels, and sessions dynamically as follows:

- 1 A remote user dials in to the ERX system (the NAS) and initiates a PPP connection to the ISP.
- 2 The ERX system and the client exchange Link Control Protocol (LCP) packets.
- 3 The NAS uses either a local database related to the domain name or RADIUS authentication to determine whether the user requires L2F service.
If the user requires L2F, the process continues.
- 4 The NAS obtains the address of the home gateway.
- 5 A tunnel is created from the NAS to the home gateway if one does not already exist. The tunnel establishment includes an ISP-to-home gateway authentication phase to protect against attack by third parties.
- 6 A new PPP connection is created in the tunnel, which in effect extends the PPP session from the remote user to the home gateway. This connection is established as follows:
The home gateway receives the LCP options and all PAP/CHAP authentication information, as negotiated by the end user and the NAS. The home gateway either accepts the connection, or it renegotiates LCP and/or reauthenticates the user.
- 7 When the NAS receives data traffic from the user, it strips the packet of framing information, encapsulates the traffic in an L2F frame, and forwards it into the tunnel.
- 8 At the home gateway, the L2F frame is removed, and the encapsulated data is forwarded into the corporate network.

References

- RFC 2341 – Cisco Layer Two Forwarding (Protocol) “L2F” (May 1998)
- *ERX Release Notes, Appendix A, System Maximums* - refer to the Release Notes corresponding to your software release for information on maximum values.

Functionality

The ERX system supports up to 200 L2F tunnels and 2,000 connections in a chassis. L2F is supported on the following modules:

- Quad-port OC3 module
- OC12 packet-over-Sonet (POS) module
- Gigabit Ethernet

The PPP session with the remote user will come in as PPPoE over ATM or PPP over ATM.

L2F Encapsulation Details

The L2F packet format contains mandatory fields that are handled in accordance with RFC 2341, which includes verifying the length of incoming L2F frames. Table 5-2 describes how the system handles optional L2F fields in the L2F header.

Table 5-2 ERX system handling of optional L2F fields

Field	Field Is Present If . . .	Description
Offset	F bit is set	<p>Indicates the number of zero-filled bytes past the L2F header where the payload starts.</p> <p>To limit the number of cache lines that must be purged during the processing of incoming UDP/IP encapsulated L2F packets, the system limits the size of L2F headers to 30 bytes. Given a maximum size of 16 bytes for the L2F header, the system will handle an offset of up to 14 bytes (more if other optional fields in the L2F header are not present). Frames with L2F headers larger than 30 bytes are silently discarded, and statistics are maintained.</p> <p>On transmission, the system always sends L2F frames with the F bit cleared and the offset omitted.</p>
Checksum	C bit is set	<p>The system accepts frames with or without checksums, but will never validate a received checksum and will never add the checksum to transmitted packets. The L2F frame is transmitted over UDP/IP, which can be configured with its own checksum. You can enable or disable UDP/IP checksum generation for L2F frames using the l2f checksum command.</p>
Key	K bit is set	<p>Contains a 32-bit value generated using the authentication response from the peer, and is used to resist attacks based on spoofing. This field is present in all but the initial L2F_CONF messages used for tunnel establishment. There is no other user control over the presence of the key field.</p>
Priority	P bit is set	<p>Distinguishes between high- and low-priority packets. The system always sets this bit to 0 (low priority) on transmitted frames and ignores this bit on received frames. The system does not set the priority bit on PPP keepalive traffic.</p>

Table 5-2 ERX system handling of optional L2F fields (continued)

Field	Field Is Present If . . .	Description
Sequence Number	S bit is set	<p>Helps to detect receipt of duplicate packets. This field must be present in all L2F management frames. It is not required in L2F data frames. However, if a data frame is received with the S bit set, all future data frames sent for that connection <i>must</i> include the sequence number.</p> <p>The system never initiates the inclusion of sequence numbers, but if it receives data frames with sequence numbers, it always responds by including sequence numbers.</p> <p>The system does not reorder sequenced data packets. It will, however, drop out-of-order sequenced data packets. For example, if packet #2 arrives before packet #1, the system forwards packet #2 and discards packet #1.</p>

Egress/Ingress Behavior

The egress interface for frames destined to the home gateway is determined by a route lookup. Therefore, the egress interface may vary on a packet-by-packet basis. This L2F implementation fixes the SA and DA on tunnel setup.

Frames transmitted from the home gateway to the ERX system may arrive on any IP interface that supports L2F. If an L2F frame arrives on an interface that does not support L2F, it is dropped.

Egress/Ingress Rate Limiting

The ERX system supports ingress and egress rate limiting on PPP traffic bound for L2F tunnels. You can apply rate limits per L2F session. To apply rate limits in this configuration, you must define an unnumbered IP interface above the PPP connection on the ingress interface. Apply rate limits to this IP interface as described in *ERX Policy and QoS Configuration Guide, Chapter 1, Configuring Policy Management*. Rate limits affect the IP-routed traffic when PPP is terminated and affect the PPP traffic when PPP is tunneled. *All* traffic is rate limited; you cannot exclude PPP control traffic.

Packet Fragmentation

The system provides reassembly of IP packets that it receives. See *ERX Routing Protocols Configuration Guide, Vol. 1, Chapter 5, IP Reassembly for Tunnels*, for more information.

The system will fragment packets entering a tunnel if the MTU for the IP egress interface is less than the total size of the encapsulated L2F packet. Identical size packets can be fragmented on some interfaces and not on others because of the egress interface determination mechanism. If the

home gateway does not support reassembly of IP packets, it may drop the fragmented packets. The UDP/IP transport handles the fragmentation.

This L2F implementation also does not support path MTU discovery. To configure your networks to avoid fragmentation when using L2F, reduce the MTU size negotiated by the PPP session. Note that the system does not enforce the MTU limit of the connection to the client on packets received from the tunnel, as it is the responsibility of the home gateway PPP session to negotiate and respect an MTU limit for all packets it originates.

AAA Support

The authentication, authorization, and accounting (AAA) server provides the means for configuring tunnels. The ERX system uses the AAA server to:

- Determine if the PPP session is to be tunneled. This step is performed by PPP during initial LCP negotiation.
- Obtain the tunneling parameters.

The AAA server performs these functions using either:

- A local database that keys off the domain name (domain-map). The domain name is identified by the remaining characters after the @ symbol in the authentication request (for example, aol.com).
- A configured RADIUS server.

In both cases, the AAA server determines if the PPP session is to be tunneled or terminated. If the PPP session is tunneled, PPP obtains the parameters detailed in Table 5-3 and returns them to L2F. Not all parameters are required.

Table 5-3 AAA tunnel parameters

Parameter	Required	IETF RADIUS Attribute	Description
HG Address	Yes	Tunnel-Server-Endpoint (67)	Indicates the address of the server end (home gateway) of the tunnel. The ERX system interprets this only as an IP address.
Tunnel Type	No	Tunnel-Type (64)	Indicates the tunneling type to be used. The ERX system will configure L2TP or L2F tunnels as indicated by this field.

Table 5-3 AAA tunnel parameters (continued)

Parameter	Required	IETF RADIUS Attribute	Description
Tunnel Medium	No	Tunnel-Medium (65)	Indicates the transport media. The ERX system supports only IP.
Tunnel Virtual Router	No	Tunnel-Virtual-Router (26-8)	Virtual router in which the tunnel is to be created.
Tunnel Authentication Password	No	Tunnel-Password (26-9)	Vendor-specific field to contain a clear-text password if the encrypted password (69) is not supported.
Tunnel Assignment	No	Tunnel-Assignment-Id (82)	Allows the ERX system to group connections into a single tunnel or create separate tunnels.
Tunnel Preference	No	Tunnel-Preference (82)	Relative priority to other tunnel definitions returned. The lower the value, the higher the preference.
Tunnel Client	No	Tunnel-Client-Auth-Id (90)	Hostname value to be used with the tunnel.

Tunnel Authentication

L2F allows for optional tunnel authentication during control connection establishment. The authentication mechanism is CHAP, which requires configuration of identical shared secrets at each peer.

If the ERX system receives a tunnel password with the tunneling parameters (see *Mapping a User Domain Name to an L2F Tunnel* later in this chapter), the system will:

- Generate a challenge during tunnel establishment.
- Be able to respond to the tunnel challenge from a home gateway during tunnel establishment.

Connection Shutdown

You can manually shut down a connection. To do this, the PPP session that performed the original proxy LCP must be shut down first. This initial step is required because, if the L2F connection is shut down first, the active PPP session could bring it right back up. See *Monitoring L2F* later in this chapter for the CLI commands to verify tunnel and connection status.

Configuring L2F

You configure tunnels using AAA server and L2F commands.



Note: In the CLI, L2F connections are referred to as sessions.

Before You Begin

Before you begin configuring your system as an NAS:

- 1 (Optional) Create a virtual router.
- 2 Assign a stable IP address, such as a loopback interface address, to the virtual router. For example:

```
host1(config)#ip router-id 198.7.3.54
```



Note: Step 2 is not necessary if you set the source-address option discussed later in this chapter.

- 3 Configure the ERX system or virtual router for B-RAS. Configuring your system for B-RAS allows it to operate as an NAS with default settings. You can modify the default settings as follows:
 - Enable the checking of data integrity via UDP.
 - Specify the time period for which the system maintains dynamic destinations, tunnels, or sessions after termination.

Mapping a User Domain Name to an L2F Tunnel

When a client initiates a PPP connection with the ERX system, the client and the system exchange LCP packets to negotiate the characteristics of the session.

To determine whether to tunnel the PPP connection using L2F, the system uses either the local database related to the user domain name or RADIUS profile information.

This section shows how to map a user domain name to an L2F tunnel. For information on setting up RADIUS to provide this mapping, see *Mapping a User Domain Name to a Virtual Router* in *Chapter 1, Configuring Remote Access to the ERX System*.

Configuration Steps

To map a domain to an L2F tunnel:

- 1 Specify a domain name.

```
host1(config)#aaa domain-map westford.com
```

- 2 Specify a virtual router. In this example, the default router is used.

```
host1(config-domain-map)#virtual-router default
```

- 3 Specify a tunnel to configure.

```
host1(config-domain-map)#tunnel 3
```

- 4 Enter the home gateway endpoint address of the tunnel.

```
host1(config-domain-map-tunnel)#address 172.31.1.98
```

- 5 Assign a preference for the tunnel.

```
host1(config-domain-map-tunnel)#preference 5
```

- 6 Assign a tunnel ID. (The system groups users with the same tunnel ID into the same tunnel.)

```
host1(config-domain-map-tunnel)#identification foo
```

- 7 Set the tunnel type to L2F.

```
host1(config-domain-map-tunnel)#type l2f
```

Optional Tasks

The following are optional parameters that you can configure.

- Assign an authentication password.

```
host1(config-domain-map-tunnel)#password dj3f92s
```

- Specify a hostname for the tunnel.

```
host1(config-domain-map-tunnel)#hostname erx4
```

- Specify a server name for the home gateway.

```
host1(config-domain-map-tunnel)#server-name boston
```

- Specify a source IP address for the NAS (ERX) tunnel endpoint.

```
host1(config-domain-map-tunnel)#source-address 170.23.2.74
```

- Specify a medium type. (Only IPv4 is supported for PPP.)

```
host1(config-domain-map-tunnel)#medium ipv4
```

- Specify a default tunnel client name.


```
host1(config-domain-map-tunnel)#exit
host1(config-domain-map)#exit
host1(config)#aaa tunnel client-name boxford
```
- Specify a default tunnel password.


```
host1(config)#aaa tunnel password 3&92k%b#q4
```
- Set up the system to ignore sequence numbers in data packets received on L2F tunnels.


```
host1(config)#l2f ignore-receive-data-sequencing
```
- Enable UDP checksums.


```
host1(config)#l2f checksum
```
- Set the idle time for tunnels and connections.


```
host1(config)#l2f destruct-timeout 1200
```
- Go to Privileged Exec mode and verify the tunnel configuration.

```
host1(config)#exit
host1#show aaa domain-map
```

```
Domain: westford; virtual-router: default
```

```
Domain: westford.com; virtual-router: default
```

Tunnel Tag	Tunnel Peer	Tunnel Source	Tunnel Type	Tunnel Medium	Tunnel Password	Tunnel Id
3	172.31.1.98	170.23.2.74	l2f	ipv4	dj3f92s	foo

Tunnel Tag	Tunnel Hostname	Tunnel Server Name	Tunnel Preference
3	erx4	boston	5

```
host1#show aaa tunnel-parameters
Tunnel password is 3&92k%b#q4
Tunnel client-name is boxford
```

aaa domain-map

- Use to specify a domain-map and enter Domain Map Configuration mode.
- Example

```
host1(config)#aaa domain-map westford.com
```
- Use the **no** version to delete the domain map.

aaa tunnel client-name

- Use to specify a default tunnel client name. If the tunnel client name is not included in the tunnel attributes that are returned from the domain map or authentication server, the system uses the default name.
- Example

```
host1(config)#aaa tunnel client-name boxford
```
- Use the **no** version to delete the client name.

aaa tunnel password

- Use to specify a default tunnel password. If the tunnel password is not included in the tunnel attributes that are returned from the domain map or authentication server, the system uses the default password.
- Example

```
host1(config)#aaa tunnel password 3&92k%b#q4
```
- Use the **no** version to delete the tunnel password.

address

- Use to set the home gateway endpoint address of a tunnel.
- Example

```
host1(config-domain-map-tunnel)#address 172.31.1.98
```
- Use the **no** version to remove the address of the tunnel.

hostname

- Use to specify the hostname that your system uses when communicating to the home gateway about the tunnel.
- The hostname is sent to the home gateway.
- Example

```
host1(config-domain-map-tunnel)#hostname erx4
```
- Use the **no** version to remove the hostname.



Note: If the home gateway does not accept tunnels from unknown hosts, the hostname must be specified in order to establish a tunnel. If no hostname is specified, the home gateway uses the system name as the hostname.

identification

- Use to specify the ID of a tunnel.
- The system groups users with the same tunnel ID in the same tunnel. This occurs only when both the destination (virtual router, IP address) and the ID are the same.
- Example

```
host1(config-domain-map-tunnel)#identification foo
```
- Use the **no** version to remove the assignment ID from the tunnel.

l2f ignore-receive-data-sequencing

- Use to prevent sequence number checking for data packets received on all L2F tunnels in the system. This command does not affect the insertion of sequence numbers in packets sent from the system.
- It is recommended that you set up the system to ignore sequence numbers in received data packets if you are using IP reassembly. Because IP reassembly may reorder L2F packets, out-of-order packets may be dropped if sequence numbers are being used on L2F data packets.
- Example

```
host1(config)#l2f ignore-receive-data-sequencing
```
- Use the **no** version to cause the system to check sequence numbers on received L2F data packets.

medium ipv4

- Use to specify the type of medium for a tunnel.
- The only medium type supported for this release is IPv4.
- Example

```
host1(config-domain-map-tunnel)#medium ipv4
```
- Use the **no** version to set the medium to the default, IPv4.

password

- Use to specify the password for a tunnel.
- If you specify a password, the same password must be configured at both the NAS and the home gateway.
- Example

```
host1(config-domain-map-tunnel)#password dj3f92s
```
- Use the **no** version to remove the password from the tunnel.

preference

- Use to specify the preference level for a tunnel.
- You can specify up to eight levels of preference.
- You can assign the same preference to a maximum of eight tunnels.

- When you define multiple preferences for a destination, you increase the probability of a successful connection.
- Example

```
host1(config-domain-map-tunnel)#preference 5
```
- Use the **no** version to set the preference number from the tunnel to the default, 0.

server-name

- Use to specify the hostname expected from the home gateway during tunnel startup. If you specify the server name, the peer must identify itself with this name during tunnel startup. Otherwise, the tunnel is closed.
- Example

```
host1(config-domain-map-tunnel)#server-name boston
```
- Use the **no** version to remove the server name.

source-address

- Use to specify the address of the local tunnel endpoint.
- When this address is specified, all L2F packets transmitted to the peer use this address.
- If this address is not specified, the virtual router's IP address is used.
- You should use the address of a stable IP interface (for example, a loopback interface). The address should also be an IP address in the specified virtual router for this domain map.
- Example

```
host1(config-domain-map-tunnel)#source-address 170.23.2.74
```
- Use the **no** version to remove the source address.

tunnel

- Use to specify a tunnel and to enter Domain Map Tunnel Configuration mode.
- Example

```
host1(config-domain-map)#tunnel 3
```
- Use the **no** version to delete the tunnel configuration.

type

- Use to specify the type of tunnel as L2F.
- Example

```
host1(config-domain-map-tunnel)#type l2f
```
- Use the **no** version to set the tunnel type to the default, L2TP.

Managing L2F

When the system has established destinations, tunnels, and sessions, you can control and manage L2F traffic as follows:

- Prevent the creation of new sessions, tunnels, and destinations.
- Close and reopen all or selected destinations, tunnels, and sessions.
- Enable UDP checksums.
- Set the idle time for which the system keeps database entries for tunnels and connections.

Making a change to a destination affects all tunnels and sessions to that destination; making a change to a tunnel affects all sessions in that tunnel. For example, closing a destination closes all tunnels and sessions to that destination.

The following commands allow you to perform these functions.

I2f checksum

- Use to enable the checking of data integrity of L2F frames using UDP checksums.
- Example

```
host1(config)#i2f checksum
```
- Use the **no** form to disable UDP checksum (the default).

I2f destruct-timeout

- Use to set the idle time, in the range 10–3600 seconds (1 hour), for which the ERX system keeps database entries for tunnels and connections.
- Example

```
host1(config)#i2f destruct-timeout 1200
```
- Use the **no** form to set this time to the default, 600 seconds.

I2f drain

- Use to prevent the creation of new destinations, tunnels, and sessions on the system.
- This command works with the **I2f shutdown** command. Both commands affect the administrative state of L2F on the system. The **I2f drain** command sets the administrative state to drain.
- Example

```
host1(config)#i2f drain
```
- Use the **no** version to enable the creation of new destinations, tunnels, and sessions.

I2f drain destination

- Use to prevent the creation of new tunnels and sessions at a destination.
- This command works with the **I2f shutdown destination** command. Both commands affect the administrative state of L2F for the destination. The **I2f drain destination** command sets the administrative state to drain.
- Example

```
host1(config)#I2f drain destination ip 172.31.1.98
```
- Use the **no** version to enable the creation of tunnels and sessions for a destination.

I2f drain tunnel

- Use to prevent the creation of new sessions for a tunnel.
- This command works with the **I2f shutdown tunnel** command. Both commands affect the administrative state of L2F for the tunnel. The **I2f drain tunnel** command sets the administrative state to drain.
- Example

```
host1(config)#I2f drain tunnel virtual-router default ip
10.3.2.1 isp.com
```
- Use the **no** version to enable the creation of a tunnel.

I2f shutdown

- Use to close all destinations, tunnels, and sessions, and to prevent the creation of new destinations, tunnels, and connections on the system.
- This command works with the **I2f drain** command. Both commands affect the administrative state of L2F on the system. The **I2f shutdown** command sets the administrative state to disabled.
- Example

```
host1(config)#I2f shutdown
```
- Use the **no** version to enable the creation of new destinations, tunnels, and sessions.

I2f shutdown destination

- Use to close all tunnels and sessions for a destination and prevent the creation of tunnels and sessions for that destination.
- This command works with the **I2f drain destination** command. Both commands affect the administrative state of the L2F on the system. The **I2f shutdown destination** command sets the administrative state to disabled.
- Example

```
host1(config)#I2f drain destination ip 10.3.2.1
```
- Use the **no** version to enable the creation of new tunnels and sessions for a destination.

l2f shutdown session

- Use to close selected sessions.
- Example

```
host1(config)#l2f shutdown session virtual-router default ip
10.2.2.1 user3
```
- The **no** version has no effect because sessions can only be created dynamically.

l2f shutdown tunnel

- Use to close all sessions in a tunnel and prevent the creation of sessions in a tunnel.
- This command works with the **l2f drain tunnel** command. Both commands affect the administrative state of L2F for the tunnel. The **l2f shutdown tunnel** command sets the administrative state to disabled.
- Example

```
host1(config)#l2f shutdown tunnel ip 10.3.2.1 boston
```
- Use the **no** version to enable the creation of new sessions for the tunnel.

Monitoring L2F

When you have configured L2F on your system, you can monitor the active tunnels and sessions using the L2F **show** commands.

You can use the **summary** or **detail** keywords to display aggregated statistics or detailed information per interface. There are also keywords that let you display information based on the state of a tunnel or session or based on location, such as a destination name or IP address.



Note: When a PPP interface has determined through its initial authentication that it is to be tunneled, its internal state changes to tunneled. The **show ppp interface** commands reflect this change in status.

show l2f

- Use to display global configuration and status information for L2F on the ERX system.
- Field descriptions
 - › Configuration:
 - L2F administrative state – status of L2F: enabled, disabled, drain
 - Dynamic interface destruct timeout – amount of time the system maintains dynamic destinations, tunnels, and sessions after they have closed
 - Data packet checksums – whether L2F checksum is enabled or disabled
 - Receive data sequencing – whether the system checks or ignores sequence numbers in incoming data packets

- › Sub-interfaces:
 - total – number of destinations, tunnels, and sessions that the system created
 - active – number of operational destinations, tunnels, and sessions
 - failed – number of requests that did not reach an operational state
 - auth-errors – number of requests that failed because the tunnel password was invalid
- Example

```
host1#show l2f
```

```
Configuration
```

```
L2F administrative state is enabled
```

```
Dynamic interface destruct timeout is 1200 seconds
```

```
Data packet checksums are disabled
```

```
Receive data sequencing is ignored
```

Sub-interfaces	total	active	failed	auth-errors
Destinations	0	0	0	n/a
Tunnels	0	0	0	0
Sessions	0	0	0	n/a

show l2f destination

- Use to display information about L2F destinations.
- Field descriptions
 - › L2F destination – status of each destination and the number of active tunnels and sessions to the destination
 - › Configuration:
 - Administrative state – configured status of the L2F destination: enabled, disabled, drain
 - SNMP traps – indicates whether or not the system is set up to send traps to SNMP for operational state changes
 - › Destination address:
 - Transport – method used to transfer traffic
 - Virtual router – name of the virtual router on which the tunnel is configured
 - Local and peer addresses – addresses of the local and remote ends of the tunnel
 - › Destination status:
 - Effective administrative state – the more restrictive of the ERX system and destination administrative states. This setting, rather than the administrative state of the destination, determines if the system can create new sessions or tunnels and if the sessions or tunnels are disabled for this destination.
 - › Sub-interfaces:
 - total – number of sessions or tunnels that the system created for this destination
 - active – number of operational sessions or tunnels for this destination

- failed – number of requests that did not reach an operational state for this destination
 - auth-errors – number of requests that failed because the tunnel password was invalid for this destination
- › Statistics:
- packets – number of control and data packets received and transmitted
 - octets – number of octets received in and transmitted from control and data packets
 - discards – number of received and transmitted control and data packets that were discarded
 - errors – number of received and transmitted control and data packets that contained errors

- Example 1

```
host1#show l2f destination
L2F destination 1 is Up with 1 active tunnel and 1 active session
L2F destination 2 is Up with 2 active tunnels and 3 active sessions
2 L2F destinations found
```

- Example 2

```
host1#show l2f destination detail ip 172.31.1.98
L2F destination 2 is Up with 2 active tunnels and 3 active sessions
Configuration
  Administrative state is enabled
  SNMP traps are enabled
Destination address
  Transport ipUdp
  Virtual router default
  Local address 172.31.1.99, peer address 172.31.1.98
Destination status
  Effective administrative state is enabled
Sub-interfaces  total      active      failed      auth-errors
  Tunnels       4          2           0           0
  Sessions      157        3           0           n/a
Statistics     packets      octets      discards    errors
  Control rx   19713       335439     0           0
  Control tx   19741       337767     0           0
  Data rx      21076       674490     6           0
  Data tx      21059       673932     0           0
```

show l2f destination summary

- Use to display a summary of the configured (administrative) and operational status of all L2F destinations.
- Field descriptions
 - › Administrative status:
 - enabled – there are no restrictions on the creation and operation of sessions and tunnels for this destination
 - drain – the **l2f drain destination** command was issued, which means the system will not create new sessions or tunnels to the destination
 - disabled – L2F sessions and tunnels were disabled using the **l2f shutdown destination** command. The system will not create new sessions or tunnels to this destination.
 - › Operational status:
 - up – destination is available for tunnels
 - down – destination is not available for tunnels
 - lower-down – underlying transport is unavailable; for example, you removed the virtual router
 - not-present – hardware supporting the destination is unavailable; for example, you removed a required line module
- Example

```

host1#show l2f destination summary
Administrative status  enabled  drain  disabled
                    2         0      0
Operational status    up       down  lower-down  not-present
                    2         0      0           0
  
```

show l2f session

- Use to display information about L2F sessions. You can display sessions for a particular tunnel or destination.
- Field descriptions
 - › Configuration:
 - Administrative state – configured status of the session: enabled or disabled
 - SNMP traps – indicates whether or not the system is set up to send traps to SNMP for operational state changes
 - › Session status:
 - Effective administrative state – the most restrictive of the following administrative states: ERX system, destination, tunnel, and session. This setting, rather than the administrative state of the session, determines whether the system can maintain this session or not.
 - State – status of the session: idle, connecting, established, disconnecting
 - Local and peer session id – names the system uses to identify the session locally and remotely

- › Statistics:
 - packets – number of control and data packets received and transmitted
 - octets – number of octets received in and transmitted from control and data packets
 - discards – number of received and transmitted control and data packets that were discarded
 - errors – number of received and transmitted control and data packets that contained errors
- › Session operational configuration – information received from the peer when the session was created

- Example 1

```
host1#show l2f session
L2F session 1/Twenty/1 is Up
L2F session 2/One/2 is Up
L2F session 2/Two/3 is LowerLayerDown
L2F session 2/Two/4 is LowerLayerDown
4 L2F sessions found
```

- Example 2

```
host1#show l2f session detail ip 172.31.1.98
L2F session 2/One/2 is Up
Configuration
  Administrative state is enabled
  SNMP traps are disabled
Session status
  Effective administrative state is enabled
  State is established
  Local session id is 5889, peer session id is 5889
Statistics      packets      octets      discards    errors
Data rx         167         5316        0           0
Data tx         161         5162        0           0
Session operational configuration
  User name is 'phil@aol.com'
  Tunneling interface atm 4/0.1
  Proxy LCP was not provided
  Authentication method was pap
1 L2F session found
```

show l2f session summary

- Use to display a summary of the configured (administrative) and operational status of all L2F sessions.
- Field descriptions
 - › Administrative status:
 - enabled – there are no restrictions on the creation of sessions
 - disabled – L2F sessions were disabled using the **l2f shutdown session** command

- › Operational status:
 - up – session is available
 - down – session is unavailable
 - lower-down – session is unavailable because the tunnel supporting the session is inaccessible
 - not-present – session is unavailable because the hardware, such as a line module, supporting the session is inaccessible

- Example

```

host1#show l2f session summary
Administrative status  enabled   disabled
                    4         0
Operational status    up        down     lower-down  not-present
                    4         0         0           0
  
```

show l2f tunnel

- Use to display detailed configuration information about specified tunnels.
- Field descriptions
 - › L2F tunnel – shows the destination/tunnel
 - › Configuration:
 - Administrative state – configured status of the L2F tunnel: enabled, disabled, drain
 - SNMP traps – indicates whether or not the system is set up to send traps to SNMP for operational state changes
 - Peer host name – hostname configured for the peer using the **server-name** command
 - Local host name – hostname configured for the ERX system end of the tunnel using the **hostname** command
 - Local address – local address configured on the tunnel
 - › Tunnel address:
 - Transport – method used to transfer traffic
 - Virtual router – name of the virtual router on which the tunnel is configured
 - Local and peer addresses – IP addresses of the local and remote ends of the tunnel
 - Local and peer UDP ports – UDP ports for the local and remote ends of the tunnel
 - › Tunnel status:
 - Effective administrative state – the most restrictive of the following administrative states: ERX system, destination, and tunnel. This setting, rather than the administrative state of the tunnel, determines whether the system can create new sessions on a tunnel or whether the sessions on a tunnel are disabled.
 - State – status of the tunnel: idle, connecting, established, disconnecting

- Local and peer tunnel id – names the system uses to identify the tunnel locally and remotely
- Last error message – last error message received on the tunnel
- › Sub-interfaces:
 - total – number of sessions that the system created for this tunnel
 - active – number of operational sessions for this tunnel
 - failed – number of requests that did not reach an operational state for this tunnel
- › Statistics:
 - packets – number of control and data packets received and transmitted
 - octets – number of octets received in and transmitted from control and data packets
 - discards – number of received and transmitted control and data packets that were discarded
 - errors – number of received and transmitted control and data packets that contained errors
- › Control channel statistics:
 - Receive out-of-sequence – number of out-of-sequence packets received on this tunnel
 - Retransmissions – number of times an L2F management packet had to be resent due to no response
- › Tunnel operational configuration – information received from the peer when the tunnel was created

- Example 1

```
host1#show l2f tunnel
L2F tunnel 1/Twenty is Up with 1 active session
L2F tunnel 2/One is Up with 1 active session
L2F tunnel 2/Two is Down with no active sessions
3 L2F tunnels found
```

- Example 2

```
host1#show l2f tunnel detail ip 172.31.1.98
L2F tunnel 2/One is Up with 1 active session
Configuration
  Administrative state is enabled
  SNMP traps are disabled
  No peer host name is configured
  Local host name is 'aolNas'
  No local address is configured
Tunnel address
  Transport ipUdp
  Virtual router default
  Local address 172.31.1.99, peer address 172.31.1.98
  Local UDP port 1701, peer UDP port 1701
Tunnel status
  Effective administrative state is enabled
```

```

State is established
Local tunnel id is 3883, peer tunnel id is 9
Last error message is 'no sessions'
Sub-interfaces total active failed
Sessions 1 1 0
Statistics packets octets discards errors
Control rx 278 4770 0 0
Control tx 278 4851 0 0
Data rx 147 4676 0 0
Data tx 141 4522 0 0
Control channel statistics
Receive out-of-sequence = 0
Retransmissions = 0
Tunnel operational configuration
Peer host name is 'aolHg'
1 L2F tunnel found

```

show l2f tunnel summary

- Use to display a summary of the configured (administrative) and operational status of all L2F tunnels.
- Field descriptions
 - › Administrative status:
 - enabled – there are no restrictions on the creation and operation of sessions for this tunnel
 - drain – the **l2f drain tunnel** command was issued, which means the system will not create new sessions for this tunnel
 - disabled – L2F tunnels were disabled using the **l2f shutdown tunnel** command. The system will not create new sessions for this tunnel.
 - › Operational status:
 - up – tunnel is available
 - down – tunnel is unavailable
 - lower-down – tunnel is unavailable because the destination supporting the tunnel is inaccessible
 - not-present – tunnel is unavailable because the hardware, such as a line module, supporting the tunnel is inaccessible
- Example

```

host1#show l2f tunnel summary
Administrative status  enabled  drain  disabled
                      3        0      0
Operational status    up      down  lower-down  not-present
                      3        0      0          0

```