14

Link Layer Discovery Protocol

Contents

Overview 14-2
LLDP 14-2
LLDP Messages 14-3
Viewing LLDP Information 14-5
Viewing LLDP Neighbor Information 14-5
Viewing Local LLDP Activity 14-8
Viewing Real-Time LLDP Messages: debug lldp Commands 14-9
Viewing LLDP Timers 14-11
Configuring LLDP 14-12
Preventing an Interface from Sending Certain LLDP Messages . . . 14-12
Preventing an Interface from Receiving LLDP Messages 14-14
Altering LLDP Timers 14-14
Quick Start 14-15

Overview

Routing protocols allow routers to learn about each other dynamically as a network expands and changes. However, these protocols run over Layer 3 of the Open Systems Interconnection (OSI) model. Devices such as switches, which operate on Layer 2, do not participate.

Networks expand all the time; switches are moved, and new ones are added. Devices need to stay up to date on these changes. Link Layer Discovery Protocol (LLDP), which runs over OSI Layer 2, allows locally attached devices in a network, such as switches and routers, to advertise information about themselves to listening devices. (See Figure 14-1.) Because devices continually broadcast and listen for LLDP messages, they can discover when a new device is added or one removed. In this way, they maintain an accurate picture of a dynamic network.

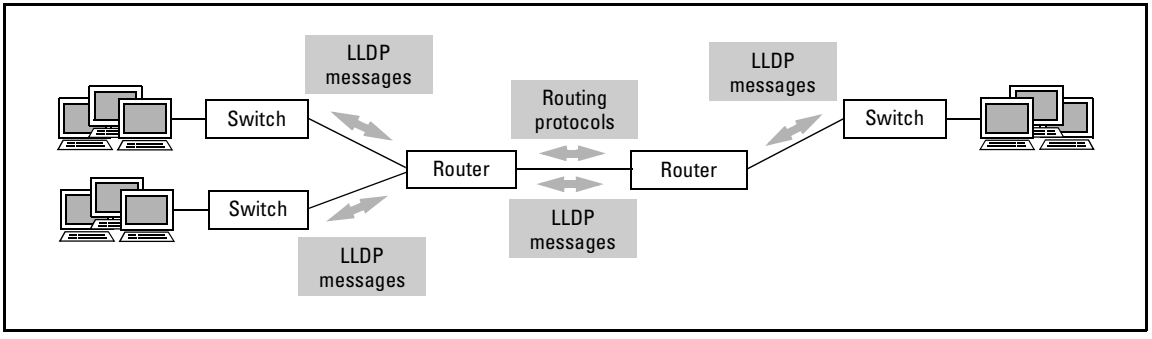

Figure 14-1. LLDP

LLDP

LLDP functions over any Data Link Layer network. Nodes transmit information about themselves and listen for information about the devices on each connection. With this information, they compile a picture of the network and of the neighbors that they can reach.

Nodes identify neighbors according to the information (such as MAC address and system name) they receive in LLDP messages. LLDP messages also include a network address where a management process such as a Simple Network Management Protocol (SNMP) server can reach the endpoint.

LLDP runs over the Data Link Layer, so devices that use different Network Layer protocols can still identify each other.

The ProCurve Secure Router automatically participates in LLDP so that the router can learn about the devices to which it connects and so that it can inform other devices of its presence.

Interfaces on the ProCurve Secure Router that run LLDP include:

- Ethernet interfaces
- Point-to-Point Protocol (PPP) interfaces
- High-level Data Link Control (HDLC) interfaces
- Frame Relay subinterfaces
- demand interfaces

LLDP Messages

Figure 14-2 illustrates the format for an LLDP message.

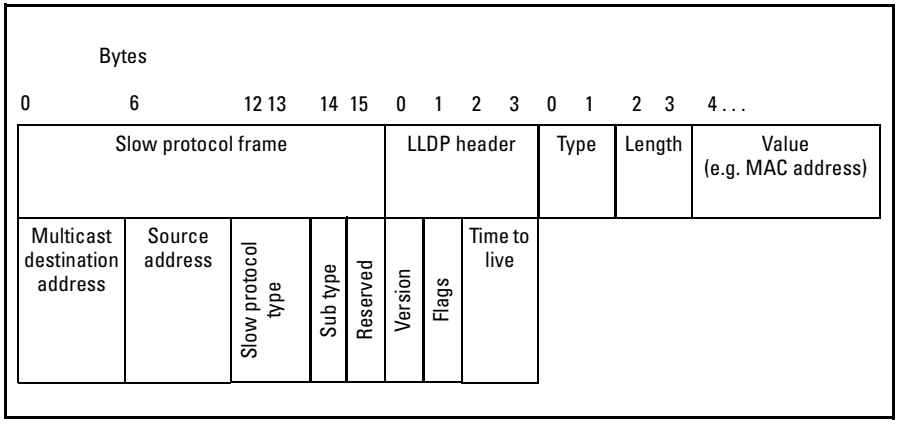

Figure 14-2. LLDP Message Sent over Ethernet

On Ethernet networks, LLDP messages are encapsulated in an 802 Slow Protocol frame, which includes a multicast destination address and the source MAC address of the transmitting interface. The Slow Protocol frame encapsulates the LLDP header and message.

Although LLDP is defined as an Ethernet protocol (802.1ab), any Layer 2 protocol can use it. ProCurve Secure Router WAN interfaces, as well as Ethernet interfaces, run LLDP.

The ProCurve Secure Router supports a network control protocol (NCP) called the LLDP Control Protocol (LLDPCP). This protocol allows PPP peers to negotiate the exchange of LLDP messages encapsulated in PPP frames.

The router can also exchange LLDP messages over a Frame Relay or an ATM PVC. A Frame Relay frame can use Sub-Network Access Protocol (SNAP) to identify encapsulated Ethernet protocols such as LLDP. ATM subinterfaces that use AAL5 Link Layer Control/ Sub-Network Access Protocol (LLC/SNAP) encapsulation similarly exchange LLDP messages. If the ATM subinterface uses AAL5 MUX encapsulation for PPP frames, then the LLDP messages can be exchanged as described for a PPP connection.

The LLDP header includes, in addition to the version field and flags, a time to live (TTL) field. The TTL informs devices how long they should store the information included in the message.

The actual information in the message consists of a type length value (TLV) field. Each TLV communicates information about the interface. The information includes:

- chassis ID—MAC address
- port ID—the interface ID (such as ppp 1)
- network address at which a management process can find the device
- system name—the device's hostname
- system description—for example, the router's model and current Secure Router OS software
- system capabilities—the device type (such as router or bridge)

You can prevent interfaces on the ProCurve Secure Router from sending some or all of these messages.

Viewing LLDP Information

The ProCurve Secure Router automatically runs LLDP with settings suitable for a typical network. Before you alter these settings, you should examine the information that the router is actually sending and receiving.

You should also understand how LLDP works so that you can capitalize on the information LLDP interfaces collect.

By scanning LLDP information, you can determine which devices the router can reach on the WAN—and whether any unauthorized devices have contacted the local router. You can also discover useful information about neighboring devices such as their capabilities and model numbers. You can also find the address for the management agents on connecting devices so that you can configure them remotely (if authorized to do so).

Viewing LLDP Neighbor Information

Each router interface listens for information from devices on the connection (its neighbor or neighbors). To view information about the router's neighbors, use this enable mode command:

Syntax: show lldp neighbors [interface <*interface ID*>] [detail]

A neighbor's LLDP information includes:

- chassis ID—MAC address
- system name—for example, a router's hostname
- port ID or device port—the ID for the neighbor interface that transmitted this message
- TTL—how long, in seconds, this information should be stored
- platform—the device model and, for the ProCurve Secure Router, the Secure Router OS version

- capabilities—all the functions the neighbor can fulfill, which include:
  - router
  - bridge
  - host
  - DOCSIS device (a type of cable modem)
  - WLAN Access Point
  - repeater
  - telephone
- enabled capabilities—the neighbor's current function; the display gives a key for the capabilities (for example, **R** for router)
- local port or interface—the interface through which the router connects to the neighbor
- management address—an IP address at which the management agent for the neighbor can be reached

Use the **detail** option to see the complete LLDP information for all neighbors. (See Figure 14-3.) For example, enter:

```
ProCurve# show lldp neighbors detail
```

If you want to limit the display to the neighbor (or, for a multi-access network, neighbors) of a specific interface, use the **interface <*interface ID*>** option. For example, enter:

```
ProCurve# show lldp neighbors interface eth 0/1 detail
```

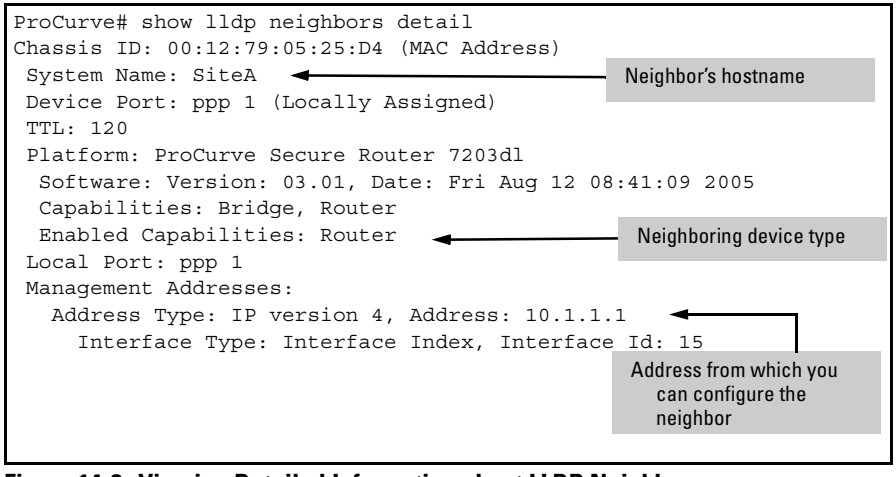

Figure 14-3. Viewing Detailed Information about LLDP Neighbors

If you enter the **show lldp neighbors** command without any options, you can also view a summary of the LLDP information. The summary includes only:

- system name
- (neighbor's) port ID
- TTL
- enabled capabilities
- platform
- local port

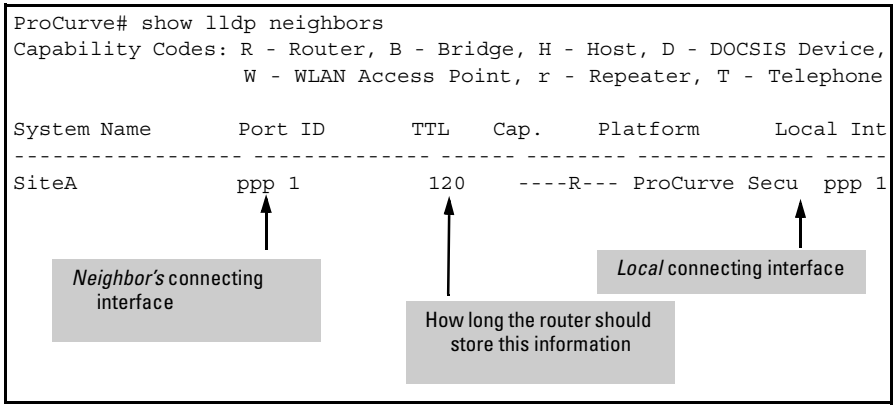

Figure 14-4. Viewing LLDP Neighbors

Figure 14-4 shows an example of the output of the **show lldp neighbors** command.

As with the detailed display, you can limit the summary to the neighbor or neighbors of a specific interface with the **interface *<interface ID>*** option. For example:

ProCurve# show lldp neighbors interface ppp 1

Alternatively, you can limit information to a specific neighbor if you know that neighbor's system name:

Syntax: show lldp device <*system name*>

A ProCurve Secure Router's system name is its hostname. For example, enter:

ProCurve# show lldp device RouterA

The **show lldp device** command automatically produces the detailed display.

You can also view actual information about neighbors as this information updates in real time. (See Figure 14-5.) Enter:

Syntax: show lldp neighbors realtime

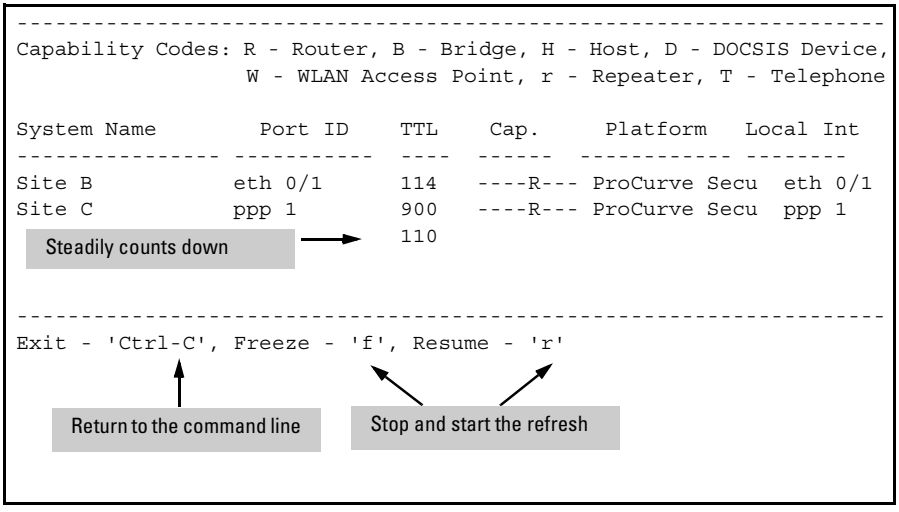

Figure 14-5. Viewing LLDP Neighbors in Real Time

If you want to view the entire LLDP message as it arrives, use the **debug lldp** commands. (See "Viewing Real-Time LLDP Messages: debug lldp Commands" on page 14-9.)

Viewing Local LLDP Activity

To see information about LLDP activity on the router, enter:

Syntax: show lldp

This command displays how often router interfaces send out LLDP and TTL packets.

To view information about the messages the router has received from, as well as transmitted to, its neighbors, enter:

Syntax: show lldp interface [<*interface ID*>]

Figure 14-6 shows the information that displays.

```
ProCurve# show lldp interface
eth 0/1 (TX/RX)
  240 packets input
    0 input errors
    0 TLV errors, 0 TLVs Discarded
    0 packets discarded
  241 packets output
  0 neighbor ageouts
fr 1.1 (TX/RX)
  235 packets input
    0 input errors
    0 TLV errors, 0 TLVs Discarded
    0 packets discarded
  235 packets output
  0 neighbor ageouts
```

Figure 14-6. Viewing LLDP Activity on Router Interfaces

The **show lldp interface** command displays the number of LLDP messages all interfaces on the local router have received (input packets) and transmitted (output packets). For the received LLDP, the command line interface (CLI) also displays the number of TLVs that had errors and that have been discarded.

When a neighbor does not send an update after the TTL for a previous message has expired, the neighbor ages out. The router assumes that endpoint no longer exists. The number of aged-out neighbors is also displayed.

You can also limit the information to a specific interface. For example:

ProCurve# show lldp interface eth 0/1

If you want to see a summary of how many neighbors the router has added and deleted, enter:

ProCurve# show lldp neighbors statistics

Viewing Real-Time LLDP Messages: debug lldp Commands

If your network is experiencing unexplained congestion, you can use the **debug** commands to explore whether a faulty interface is flooding the network with LLDP messages. You can also use the **debug lldp** commands to determine which interfaces are sending and receiving LLDP messages and what information these messages contain.

Caution Debug messages are processor intensive.

You can view the LLDP messages that are arriving on interfaces in real time by entering:

Syntax: debug lldp rx [verbose]

If an interface seems to be receiving an undue number of messages, you can enter the **show lldp neighbors interface *<interface ID>*** command to view information about the device at fault. You should then troubleshoot that device.

You can also track the LLDP activity of interfaces on the local router. To monitor the LLDP messages that the router interfaces are transmitting, enter:

Syntax: debug lldp tx [verbose]

If you want to change how often interfaces send messages, you can raise the minimum transmit interval. (See “Altering LLDP Timers” on page 14-14.)

Entering the **debug** commands without the **verbose** option simply informs you when a LLDP message is sent or received. If you want to see the actual information in the message, you should add the **verbose** option. For example:

```
ProCurve# debug lldp tx verbose
```

Figure 14-7 displays an example of the verbose debug of an LLDP message.

If you do not want the router to send the information you see displayed, or a specific portion of this information, you should prevent the interface from sending the corresponding type of LLDP message. WAN interfaces, in particular, can compromise a network by transmitting LLDP messages to an untrusted device. See “Preventing an Interface from Sending Certain LLDP Messages” on page 14-12.

```
ProCurve# debug lldp tx verbose
LLDP:   TTL 120
LLDP:   System Description "ProCurve Secure Router 7203dl"
LLDP:   System Name "ProCurve"
LLDP:   System Description "ProCurve Secure Router 7203dl, Version:
03.01, Date: Fri Aug 12 08:41:29 2005"
LLDP:    System Capabilities:
LLDP:       Bridge, Router
LLDP:    Enabled System Capabilities:
LLDP:       Router
LLDP:    Management Address:
LLDP:      Type: "IP version 4"  Address: "192.168.1.1"
LLDP:      Interface Type: "Interface Index" Id: 13
LLDP:      OID: "1.3.6.1.2.1.2.2.1.1.13"
LLDP: Next Update for eth 0/1 in 30 second
```

Figure 14-7. Debugging LLDP Messages

Viewing LLDP Timers

You can view the global settings for LLDP timers by entering this enable mode command:

Syntax: show lldp

The CLI displays:

- how often LLDP messages are sent
- how often TTL updates are sent

You can change how often LLDP messages are sent by changing the transmit interval and minimum transmit interval. You cannot directly change the TTL. Instead, you must change the TTL multiplier, which determines for how many transmit intervals a message is stored. The TTL is the transmit interval multiplied by the TTL multiplier.

See “Altering LLDP Timers” on page 14-14 to learn more about altering timers.

Configuring LLDP

All active interfaces on the ProCurve Secure Router, except for ATM subinterfaces, automatically send out LLDP messages. (See Table 14-2 on page 14-15 for the default transmit intervals.)

For most networks, the default settings for LLDP are adequate.

If you so choose, you can attempt to minimize overhead or to restrict the information the router transmits about itself by:

- preventing an interface from sending certain LLDP messages
- preventing an interface from receiving LLDP messages
- altering the intervals for sending LLDP messages

Preventing an Interface from Sending Certain LLDP Messages

By default, the ProCurve Secure Router sends LLDP messages over all Ethernet and logical interfaces except ATM subinterfaces, which do not support LLDP.

These messages include information about the interface and about the local router:

- MAC address
- port ID
- router model and Secure Router OS software version
- router's hostname
- system capabilities
- network address at which a management process can find the device

You should be cautious about the information that you allow WAN interfaces to transmit, particularly on routers that connect to an external network. An unauthorized device can learn a great deal about your system from LLDP messages.

To restrict an interface from transmitting LLDP messages, move to the configuration mode context for the interface and enter:

Syntax: no lldp send [management-address | port-description | system-capabilities | system-description | system-name]

Enter **no lldp send** without any options to prevent the interface from transmitting any messages.

You can restrict the interface from sending only certain messages by entering the **no** form of the **lldp send** command followed by the specific option. For example, if a WAN interface transmits the management address into an untrusted environment, hackers could attempt to access your router. On the other hand, sending this address to authorized management processes allows network administrators at hub sites to access and manage routers at remote sites.

Preventing interfaces from sending messages that you consider less important can minimize the protocol's chattiness.

Refer to Table 14-1 for the commands for suppressing or enabling specific types of LLDP messages.

Table 14-1. Suppressing and Enabling LLDP Messages

Message	Command Syntax
IP address for the interface's management agent	**[no] lldp send management-address**
interface's port ID	**[no] lldp send port-description**
system capabilities (for example, router or bridge)	**[no] lldp send system-capabilities**
router model and software version	**[no] lldp send system-description**
router's hostname	**[no] lldp send system-name**

LLDP messages *must* include a MAC address (chassis ID). If you do not want the interface to send its MAC address, you must prevent it from transmitting any LLDP messages.

Note Even after you prevent an interface from transmitting LLDP messages, it can still listen for them.

Preventing an Interface from Receiving LLDP Messages

You can prevent an interface from listening for LLDP messages by moving to its configuration mode context and entering:

Syntax: no lldp receive

You cannot filter out certain types of information. The interface either receives all LLDP messages or none.

Note

Preventing an interface from receiving LLDP messages does not stop it from sending them. You prevent an interface from participating in LLDP entirely with this command, entered from the interface configuration mode context:

Syntax: no lldp send-and-receive

Altering LLDP Timers

LLDP can be chatty; you can increase the intervals at which interfaces transmit messages to reduce network congestion.

The transmit interval determines how often an interface sends out LLDP messages during normal operations. However, the interface can send messages more often—for example, when its status changes. A flapping interface, which toggles between up and down, may send messages out again and again. If LLDP messages are causing too much overhead, you can force the interface to wait a set amount of time before transmitting a new message by raising the minimum transmit interval.

An LLDP header includes a TTL field that informs neighboring devices how long they should store the information in the message. The interface sets the TTL field by multiplying the transmit interval by the TTL multiplier. By default, this multiplier is four. That is, information is assumed to be accurate for four LLDP cycles.

You configure LLDP intervals for all interfaces from the global configuration mode context. Refer to Table 14-2 for the exact command syntax.

Table 14-2. LLDP Intervals

Interval	Meaning	Default	Range	Command Syntax
transmit interval	time between sending LLDP messages during normal operations	30 seconds	5 to 32,768 seconds	**lldp transmit-interval <seconds>**
minimum transmit interval	minimum time the interface must wait before sending a new LLDP message	2 seconds	1 to 8192	**lldp minimum-transmit-interval <seconds>**
ttl multiplier	number of transmit intervals information should be stored	4	2 to 10	**lldp ttl-multiplier <value>**
reinitialization delay	time an interface must wait to send an LLDP message after LLDP is re-enabled	2 seconds	1 to 10 seconds	**lldp reinitialization-delay <seconds>**

Quick Start

All Ethernet and logical interfaces on the ProCurve Secure Router, except ATM subinterfaces, automatically run LLDP. Typically, you do not need to change any configurations.

This section provides the commands you must enter to quickly:

- disable LLDP on a specific interface
- disable an interface from sending specific types of information about the router
- view information about LLDP neighbors

Only a minimal explanation is provided. If you need additional information about any of these options, check "Contents" on page 14-1 to locate the section that contains the explanation you need.

1. You can disable LLDP on a specific interface. Move to its configuration mode context and enter one or more of these commands:
   a. To disable LLDP entirely, enter:

      Syntax: no lldp send-and-receive

b. You can also prevent the router from sending any LLDP messages, while still allowing it to listen for messages.

Syntax: no lldp send

c. To only prevent the router from receiving LLDP messages, enter:

Syntax: no lldp receive

Enter a command without the **no** option to re-enable the function.

2. You can prohibit an interface from sending some kinds of information about the router, but allow it to send other information. Move to the interface's configuration mode context. Then enter this command followed by the keyword for the type of information that you want to restrict:

Syntax: no lldp send [management-address | port-description | system-capabilities | system-description | system-name]

Table 14-3 explains what information is associated with each keyword.

Enter the command without the **no** option to re-enable the router to send that information.

Table 14-3. Prohibiting an Interface from Sending Certain LLDP Messages

Keyword	Information
management-address	IP address at which a management process can reach the router
port-description	interface's port ID
system-capabilities	system's capabilities (for example, router or bridge)
system-description	router model and software version
system-name	router's hostname

3. To view information about the router's neighbors, move to the global configuration mode context and enter:

Syntax: show lldp neighbors [interface <*interface ID*>] [detail]

Use the **interface <*interface ID*>** option to view information about only a specific interface's neighbor. The **detail** option displays all LLDP information.

4. To view information about a specific device, enter:

Syntax: show lldp device <*system name*>