

Configuring for Network Management Applications

Contents

Using SNMP Tools To Manage the Switch	14-3
Overview	14-3
SNMP Management Features	14-4
Configuring for SNMP version 1 and 2c Access to the Switch	14-4
Configuring for SNMP Version 3 Access to the Switch	14-5
SNMP Version 3 Commands	14-6
Enabling SNMPv3	14-7
SNMPv3 Users	14-7
Group Access Levels	14-11
SNMPv3 Communities	14-11
Menu: Viewing and Configuring non-SNMP version 3 Communities	14-13
CLI: Viewing and Configuring SNMP Community Names	14-15
SNMP Notifications	14-17
Supported Notifications	14-17
General Steps for Configuring SNMP Notifications	14-18
SNMPv1 and SNMPv2c Traps	14-19
Configuring an SNMP Trap Receiver	14-19
Enabling SNMPv2c Informs	14-21
Configuring SNMPv3 Notifications	14-23
Managing Network Security Notifications	14-26
Enabling Link-Change Traps	14-28
Configuring the Source IP Address for SNMP Notifications ..	14-29
Displaying SNMP Notification Configuration	14-31
Advanced Management: RMON	14-33
CLI-Configured sFlow with Multiple Instances	14-33

Terminology	14-33
Configuring sFlow	14-34
Viewing sFlow Configuration and Status	14-34
LLDP (Link-Layer Discovery Protocol)	14-37
Terminology	14-38
General LLDP Operation	14-40
LLDP-MED	14-40
Packet Boundaries in a Network Topology	14-40
Configuration Options	14-41
Options for Reading LLDP Information Collected by the Switch ..	14-43
LLDP and LLDP-MED Standards Compatibility	14-43
LLDP Operating Rules	14-44
Configuring LLDP Operation	14-45
Viewing the Current Configuration	14-45
Configuring Global LLDP Packet Controls	14-47
Configuring SNMP Notification Support	14-51
Configuring Per-Port Transmit and Receive Modes	14-52
Configuring Basic LLDP Per-Port Advertisement Content	14-53
Configuring Support for Port Speed and Duplex Advertisements	14-55
LLDP-MED (Media-Endpoint-Discovery)	14-56
LLDP-MED Topology Change Notification	14-59
LLDP-MED Fast Start Control	14-61
Advertising Device Capability, Network Policy, PoE Status and Location Data	14-61
Configuring Location Data for LLDP-MED Devices	14-65
Displaying Advertisement Data	14-70
Displaying Switch Information Available for Outbound Advertisements	14-71
Displaying LLDP Statistics	14-75
LLDP Operating Notes	14-77
LLDP and CDP Data Management	14-79
LLDP and CDP Neighbor Data	14-79
CDP Operation and Commands	14-81

Using SNMP Tools To Manage the Switch

Overview

You can manage the switch via SNMP from a network management station running an application such as ProCurve Manager (PCM) or ProCurve Manager Plus (PCM+). For more on PCM and PCM+, visit the ProCurve Networking web site at:

www.procurve.com

Click on **products index** in the sidebar, then click on the appropriate link appearing under the **Network Management** heading.

This section includes:

- An overview of SNMP management for the switch
- Configuring the switches for:
 - SNMP Communities (page 14-11)
 - Trap Receivers and Authentication Traps (page 14-17)
- Information on advanced management through RMON Support (page 14-33)

To implement SNMP management, the switch must have an IP address, configured either manually or dynamically (using DHCP or Bootp). If multiple VLANs are configured, each VLAN interface should have its own IP address. For DHCP use with multiple VLANs, refer to the section titled “The Primary VLAN” in the “Static Virtual LANs (VLANs)” chapter of the *Advanced Traffic Management Guide* for your switch.

Note

If you use the switch’s Authorized IP Managers and Management VLAN features, ensure that the SNMP management station and/or the choice of switch port used for SNMP access to the switch are compatible with the access controls enforced by these features. Otherwise, SNMP access to the switch will be blocked. For more on Authorized IP Managers, refer to the *Access Security Guide* for your switch. (The latest version of this guide is available on the ProCurve Networking web site.) For information on the Management VLAN feature, refer to the section titled “The Secure Management VLAN” in the “Static Virtual LANs (VLANs)” chapter of the *Advanced Traffic Management Guide* for your switch.

SNMP Management Features

SNMP management features on the switch include:

- SNMP version 1, version 2c, or version 3 over IP
- Security via configuration of SNMP communities (page 14-11)
- Security via authentication and privacy for SNMP Version 3 access
- Event reporting via SNMP
 - Version 1 traps
 - RMON: groups 1, 2, 3, and 9
- ProCurve Manager/Plus support
- Flow sampling using sFlow
- Standard MIBs, such as the Bridge MIB (RFC 1493), Ethernet MAU MIB (RFC 1515), and others.

The switch SNMP agent also uses certain variables that are included in a Hewlett-Packard proprietary MIB (Management Information Base) file. If you are using HP OpenView, you can ensure that it is using the latest version of the MIB file by downloading the file to the OpenView database. To do so, go to the ProCurve Networking web site at:

www.procurve.com

Click on **software updates**, then **MIBs**.

Configuring for SNMP version 1 and 2c Access to the Switch

SNMP access requires an IP address and subnet mask configured on the switch. (Refer to “IP Configuration” on page 8-2.) If you are using DHCP/Bootp to configure the switch, ensure that the DHCP/Bootp process provides the IP address. (Refer to “DHCP/Bootp Operation” on page 8-12.)

Once an IP address has been configured, the main steps for configuring SNMP version 1 and version 2c access management features are:

1. Configure the appropriate SNMP communities. (Refer to “SNMPv3 Communities” on page 14-11.)
2. Configure the appropriate trap receivers. (Refer to “SNMP Notifications” on page 14-17.)

In some networks, authorized IP manager addresses are not used. In this case, all management stations using the correct community name may access the switch with the View and Access levels that have been set for that community.

If you want to restrict access to one or more specific nodes, you can use the switch's IP Authorized Manager feature. (Refer to the *Access Security Guide* for your switch.)

Caution

For ProCurve Manager (PCM) version 1.5 or earlier (or any TopTools version), deleting the “public” community disables some network management functions (such as traffic monitoring, SNMP trap generation, and threshold setting). If network management security is a concern, and you are using the above software versions, ProCurve recommends that you change the write access for the “public” community to “Restricted”.

Configuring for SNMP Version 3 Access to the Switch

SNMP version 3 (SNMPv3) access requires an IP address and subnet mask configured on the switch. (Refer to “IP Configuration” on page 8-2.) If you are using DHCP/Bootp to configure the switch, ensure that the DHCP/Bootp process provides the IP address. (See “DHCP/Bootp Operation” on page 8-12.)

Once an IP address has been configured, the main steps for configuring SNMP version 3 access management features are:

1. Enable SNMPv3 for operation on the switch (Refer to “SNMP Version 3 Commands” on page 14-6)
2. Configure the appropriate SNMP users (Refer to “SNMPv3 Users” on page 14-7)
3. Configure the appropriate SNMP communities. (Refer to “SNMPv3 Communities” on page 14-11.)
4. Configure the appropriate trap receivers. (Refer to “SNMP Notifications” on page 14-17.)

In some networks, authorized IP manager addresses are not used. In this case, all management stations using the correct User and community name may access the switch with the View and Access levels that have been set for that community. If you want to restrict access to one or more specific nodes, you can use the switch's IP Authorized Manager feature. (Refer to the *Access Security Guide* for your switch.)

SNMP Version 3 Commands

SNMP version 3 (SNMPv3) adds some new commands to the CLI for configuring SNMPv3 functions. To enable SMNPv3 operation on the switch, use the **snmpv3 enable** command. An initial user entry will be generated with MD5 authentication and DES privacy.

You may (optionally) restrict access to only SNMPv3 agents by using the **snmpv3 only** command. To restrict write-access to only SNMPv3 agents, use the **snmpv3 restricted-access** command.

Caution

Restricting access to only version 3 messages will make the community named “public” inaccessible to network management applications (such as auto-discovery, traffic monitoring, SNMP trap generation, and threshold setting) from operating in the switch.

Syntax: [no] snmpv3 enable

Enable and disable the switch for access from SNMPv3 agents. This includes the creation of the initial user record.

[no] snmpv3 only

Enables or disables restrictions to access from only SNMPv3 agents. When enabled, the switch will reject all non-SNMPv3 messages.

[no] snmpv3 restricted-access

Enables or disables restrictions from all non-SNMPv3 agents to read only access.

show snmpv3 enable

Displays the operating status of SNMPv3.

show snmpv3 only

Displays status of message reception of non-SNMPv3 messages.

show snmpv3 restricted-access

Displays status of write messages of non-SNMPv3 messages.

Enabling SNMPv3

The **snmpv3 enable** command allows the switch to:

- Receive SNMPv3 messages.
- Configure initial users.
- Restrict non-version 3 messages to “read only” (optional).

Figure 14-1 shows an example of how to use the **snmpv3 enable** command.

Note:
SNMP
Version 3
Initial Users

To create new users, most SNMPv3 management software requires an initial user record to clone. The initial user record can be downgraded and provided with fewer features, but not upgraded by adding new features. For this reason it is recommended that when you enable SNMPv3, you also create a second user with SHA authentication and DES privacy.

```
ProCurve (config)# snmpv3 enable
SNMPv3 Initialization process.
Creating user 'initial'
Authentication Protocol: MD5
Enter authentication password: *****
Privacy protocol is DES
Enter privacy password: *****

User 'initial' is created
Would you like to create a user that uses SHA? y
Enter user name: templateSHA
Authentication Protocol: SHA
Enter authentication password: *****
Privacy protocol is DES
Enter privacy password: *****

User creation is done.  SNMPv3 is now functional.
Would you like to restrict SNMPv1 and SNMPv2c messages to have read only
access (you can set this later by the command 'snmp restrict-access'): n
```

The diagram shows three callout boxes with arrows pointing to specific lines in the terminal output:

- Enable SNMPv3**: Points to the `snmpv3 enable` command.
- Create initial user models for SNMPv3 Management Applications**: Points to the user creation process, including the creation of the 'initial' user and the 'templateSHA' user.
- Set restriction on non-SNMPv3 messages**: Points to the final question about restricting SNMPv1 and SNMPv2c messages.

Figure 14-1. Example of SNMP version 3 Enable Command

SNMPv3 Users

To use SNMPv3 on the switch, you must configure the users that will be assigned to different groups. To configure SNMP users on the switch:

1. Configure users in the User Table with the **snmpv3 user** command. To view the list of configured users, enter the **show snmpv3 user** command (see “Adding Users” on page 14-8).
2. Assign users to Security Groups based on their security model with the **snmpv3 group** command (see “Assigning Users to Groups” on page 14-10).

Caution

If you add an SNMPv3 user without authentication and/or privacy to a group that requires either feature, the user will not be able to access the switch. Ensure that you add a user with the appropriate security level to an existing security group.

Adding Users. To configure an SNMPv3 user, you must first add the user name to the list of known users with the **snmpv3 user** command.

```
ProCurve(config)# snmpv3 user NetworkAdmin
ProCurve(config)# snmpv3 user NetworkMgr auth md5 authpass priv privpass
ProCurve(config)# show snmpv3 user
```

Status and Counters - SNMP v3 Global Configuration Information

User Name	Auth. Protocol	Privacy Protocol
initial	MD5	CFB AES-128
NetworkAdmin	MD5	CBC-DES

Figure 14-2. Adding SNMPv3 Users and Displaying SNMPv3 Configuration

SNMPv3 User Commands

Syntax: [no] snmpv3 user <user_name>

Adds or deletes a user entry for SNMPv3. Authorization and privacy are optional, but to use privacy, you must use authorization. When you delete a user, only the <user_name> is required.

[auth <md5 | sha> <auth_pass>]

*With authorization, you can set either MD5 or SHA authentication. The authentication password <auth_pass> must be 6-32 characters in length and is mandatory when you configure authentication.
Default: None*

[priv <des | aes> <priv_pass>]

*With privacy, the switch supports DES (56-bit) and AES (128-bit) encryption. The privacy password <priv_pass> must be 6-32 characters in length and is mandatory when you configure privacy.
Default: DES*

Note: *Only AES 128-bit and DES 56-bit encryption are supported as privacy protocols. Other non-standard encryption algorithms, such as AES-172, AES-256, and 3-DES are not supported.*

Listing Users. To display the management stations configured to access the switch with SNMPv3 and view the authentication and privacy protocols that each station uses, enter the **show snmpv3 user** command.

Syntax: show snmpv3 user

This example displays information about the management stations configured on VLAN 1 to access the switch.

```
ProCurve# configure terminal
ProCurve(config)# vlan 1
ProCurve(vlan-1)# show snmpv3 user

Status and Counters - SNMPv3 Global Configuration Information

User Name          Auth. Protocol      Privacy Protocol
-----
initial            MD5                 CFB AES-128
NetworkAdmin       MD5                 CBC-DES
```

Assigning Users to Groups. Then you must set the group access level for the user by assigning the user to a group. This is done with the **snmpv3 group** command. For more details on the MIBs access for a given group refer to “Group Access Levels” on page 14-11.

The screenshot shows a configuration session on a switch. Two commands are entered to assign users to groups:

```
ProCurve.(config)# snmpv3 group operatornoauth user NetworkAdmin sec-model ver3
ProCurve.(config)# snmpv3 group managerpriv user NetworkMgr sec-model ver3
```

The 'show snmpv3 group' command displays the following configuration:

```
ProCurve.(config)# show snmpv3 group

Status and Counters - SNMP v3 Global Configuration Information

-----
Security Name                Security Model  Group Name
-----
CommunityManagerReadOnly    ver1           ComManagerR
CommunityManagerReadWrite    ver1           ComManagerRW
CommunityOperatorReadOnly    ver1           ComOperatorRW
CommunityOperatorReadWrite    ver1           ComOperatorRW
CommunityManagerReadOnly     ver2c          ComManagerR
CommunityManagerReadWrite     ver2c          ComManagerRW
CommunityOperatorReadOnly     ver2c          ComOperatorRW
CommunityOperatorReadWrite    ver2c          ComOperatorRW
NetworkMgr                   ver3           ManagerPriv
NetworkAdmin                 ver3           OperatorNoAuth
```

Annotations in the image:

- An arrow points from the text "Add NetworkAdmin to operator noauth group" to the first configuration line.
- An arrow points from the text "Add NetworkMgr to managerpriv group" to the second configuration line.
- An arrow points from the text "Pre-assigned groups for access by Version 2c and version 1 management applications" to the 'CommunityOperatorReadWrite' entry in the table.

Figure 14-3. Example of Assigning Users to Groups

SNMPv3 Group Commands

Syntax: [no] snmpv3 group

This command assigns or removes a user to a security group for access rights to the switch. To delete an entry, all of the following three parameters must be included in the command.

group <group_name>

This parameter identifies the group that has the privileges that will be assigned to the user. For more details refer to “Group Access Levels” on page 14-11.

user <user_name>

*This parameter identifies the user to be added to the access group. This must match the user name added with the **snmpv3 user** command.*

sec-model <ver1 | ver2c | ver3>

This defines which security model to use for the added user. A SNMPv3 access Group should only use the ver3 security model.

Group Access Levels

The switch supports eight predefined group access levels. There are four levels for use with version 3 users and four are used for access by version 2c or version 1 management applications.

Group Name	Group Access Type	Group Read View	Group Write View
managerpriv	Ver3 Must have Authentication and Privacy	ManagerReadView	ManagerWriteView
managerauth	Ver3 Must have Authentication	ManagerReadView	ManagerWriteView
operatorauth	Ver3 Must have Authentication	OperatorReadView	DiscoveryView
operatornoauth	Ver3 No Authentication	OperatorReadView	DiscoveryView
commanagerrw	Ver2c or Ver1	ManagerReadView	ManagerWriteView
commanagerr	Ver2c or Ver1	ManagerReadView	DiscoveryView
comoperatorrw	Ver2c or Ver1	OperatorReadView	OperatorReadView
comoperatorr	Ver2c or Ver1	OperatorReadView	DiscoveryView

Each view allows you to view or modify a different set of MIBs.

- **Manager Read View** – access to all managed objects
- **Manager Write View** – access to all managed objects *except* the following: vacmContextTable, vacmAccessTable, vacmViewTreeFamilyTable
- **OperatorReadView** – no access to icfSecurityMIB, hpSwitchIpTftp-Mode, vacmContextTable, vacmAccessTable, vacmViewTreeFamilyTable, usmUserTable, snmpCommunityTable
- **Discovery View** – Access limited to samplingProbe MIB.

Note

All access groups and views are predefined on the switch. There is no method to modify or add groups or views to those that are pre-defined on the switch.

SNMPv3 Communities

SNMP communities are supported by the switch to allow management applications that use version 2c or version 1 to access the switch. The communities are mapped to Group Access Levels that are used for version 2c or version 1 support. For more information refer to “Group Access Levels” on page 14-11. This mapping will happen automatically based on the communities access privileges, but special mappings can be added with the **snmpv3 community** command.

Syntax: [no] snmpv3 community

*This command maps or removes a mapping of a community name to a group access level. To remove a mapping you, only need to specify the **index_name** parameter.*

index <index_name>

This is an index number or title for the mapping. The values of 1-5 are reserved and can not be mapped.

name <community_name>

This is the community name that is being mapped to a group access level.

sec-name <security_name>

This is the group level to which the community is being mapped. For more information refer to “Group Access Levels” on page 14-11.

tag <tag_value>

This is used to specify which target address may have access by way of this index reference.

Figure 14-4 shows the assigning of the Operator community on MgrStation1 to the CommunityOperatorReadWrite group. Any other Operator only has an access level of CommunityOperatorReadOnly

Add mapping to allow write access for Operator community on MgrStation1

```

ProCurve (config)# snmpv3 community index 30 name Operator sec-name
CommunityManagerReadWrite tag MgrStation1
ProCurve (config)# show snmpv3 community
    
```

Two Operator Access Levels

Index Name	Community Name	Security Name
1	public	CommunityManagerReadWrite
2	Operator	CommunityOperatorReadOnly
3	Manager	CommunityManagerReadWrite
30	Operator	CommunityManagerReadWrite

Figure 14-4. Assigning a Community to a Group Access Level

SNMP Community Features

Feature	Default	Menu	CLI	Web
show SNMP communities	n/a	page 14-13	page 14-15	—
configure identity information	none	—	page 14-16	
configure community names	public	page 14-13	page 14-16	—
MIB view for a community name (operator, manager)	manager	"	"	
write access for default community name	unrestricted	"	"	

Use SNMP communities to restrict access to the switch by SNMP management stations by adding, editing, or deleting SNMP communities. You can configure up to five SNMP communities, each with either an operator-level or a manager-level view, and either restricted or unrestricted write access.

Using SNMP requires that the switch have an IP address and subnet mask compatible with your network.

Caution

For ProCurve Manager (PCM) version 1.5 or earlier (or any TopTools version), deleting the “public” community disables some network management functions (such as traffic monitoring, SNMP trap generation, and threshold setting). If network management security is a concern, and you are using the above software versions, ProCurve recommends that you change the write access for the “public” community to “Restricted”.

Menu: Viewing and Configuring non-SNMP version 3 Communities

To View, Edit, or Add SNMP Communities:

1. From the Main Menu, Select:
 2. **Switch Configuration...**
 6. **SNMP Community Names**

Configuring for Network Management Applications

Using SNMP Tools To Manage the Switch

Note: This screen gives an overview of the SNMP communities that are currently configured. All fields in this screen are read-only.

```

===== CONSOLE - MANAGER MODE =====
Switch Configuration - SNMP Communities

Community Name  MIB View  Write Access
-----
public          Manager   Unrestricted

Actions->  Back    Add    Edit    Delete    Help

Return to previous screen.
Use up/down arrow keys to change record selection, left/right arrow ke
  
```

Add and Edit options are used to modify the SNMP options. See Figure 8-2.

Figure 14-5. The SNMP Communities Screen (Default Values)

2. Press **[A]** (for **Add**) to display the following screen:

If you are adding a community, the fields in this screen are blank.

If you are editing an existing community, the values for the currently selected Community appear in the fields.

```

===== CONSOLE - MANAGER MODE =====
Switch Configuration - SNMP Communities

Community Name : 
MIB View : Manager

Write Access : Restricted

Actions->  Cancel  Edit  Save  Help

Enter Community Name - up to 16 characters, case sensitive; no spaces
Use arrow keys to change field selection, <Space> to toggle field choi
  
```

Type the value for this field.
Use the Space bar to select values for other fields

Figure 14-6. The SNMP Add or Edit Screen

Need Help? If you need information on the options in each field, press **[Enter]** to move the cursor to the Actions line, then select the **H**elp option on the Actions line. When you are finished with Help, press **[E]** (for **E**dit) to return the cursor to the parameter fields.

3. Enter the name you want in the Community Name field, and use the Space bar to select the appropriate value in each of the other fields. (Use the **[Tab]** key to move from one field to the next.)
4. Press **[Enter]**, then **[S]** (for **S**ave).

CLI: Viewing and Configuring SNMP Community Names

Community Name Commands	Page
show snmp-server [<i><community-string></i>]	14-15
[no] snmp-server	14-16
[community <i><community-str></i>]	14-16
[host <i><community-str></i> <i><ip-addr></i>] [<i><none debug all not-info critical></i>]	14-19
[enable traps <i><authentication></i>]	14-27
[enable traps link-change <i><port-list></i>]	14-28

Listing Community Names and Values. This command lists the data for currently configured SNMP community names (along with trap receivers and the setting for authentication traps — refer to “SNMP Notifications” on page 14-17).

Syntax: show snmp-server [*<community-string>*]

This example lists the data for all communities in a switch; that is, both the default “public” community name and another community named “blue-team”

```

ProCurve# show snmp-server

SNMP Communities

Community Name  MIB View  Write Access
-----
public         Manager   Unrestricted
blue-team      Operator  Restricted

Trap Receivers

Send Authentication Traps [No] : No

Address                Community          Events Sent in Trap
-----

```

Figure 14-7. Example of the SNMP Community Listing with Two Communities

To list the data for only one community, such as the “public” community, use the above command with the community name included. For example:

```
ProCurve# show snmp-server public
```

Configuring Community Names and Values. The **snmp-server** command enables you to add SNMP communities with either default or specific access attributes, and to delete specific communities.

Syntax: [no] snmp-server community < community-name >

Configures a new community name. If you do not also specify **operator** or **manager**, the switch automatically assigns the community to the **operator** MIB view. If you do not specify **restricted** or **unrestricted**, the switch automatically assigns the community to **restricted** (read-only) access. The **no** form uses only the < **community-name** > variable and deletes the named community from the switch.

[operator | manager]

*Optionally assigns an access level. At the **operator** level the community can access all MIB objects except the CONFIG MIB. At the **manager** level the community can access all MIB objects.*

[restricted | unrestricted]

*Optionally assigns MIB access type. Assigning the **restricted** type allows the community to read MIB variables, but not to set them. Assigning the **unrestricted** type allows the community to read and set MIB variables.*

For example, to add the following communities:

Community	Access Level	Type of Access
red-team	manager <i>(Access to all MIB objects.)</i>	unrestricted <i>(read/write)</i>
blue-team	operator <i>(Access to all MIB objects except the CONFIG MIB.)</i>	restricted <i>(read-only)</i>

```
ProCurve(config)# snmp-server community red-team  
manager unrestricted  
ProCurve(config)# snmp-server community blue-team  
operator restricted
```

To eliminate a previously configured community named "gold-team":

```
ProCurve(config) # no snmp-server community gold-team
```


SNMP Notifications

The switches covered in this guide support:

- SNMP version 1 or SNMP version 2c traps
- SNMPv2c informs
- SNMPv3 notification process, including traps

This section describes how to configure a switch to send network security and link-change notifications to configured trap receivers.

Supported Notifications

By default, the following notifications are enabled on a switch:

- Manager password changes
- SNMP authentication failure
- Link-change traps: when the link on a port changes from up to down (linkDown) or down to up (linkUp)
- Port-security (web, MAC, or 802.1X) authentication failure
- Invalid password entered in a login attempt through a direct serial, Telnet, or SSH connection
- Inability to establish a connection with the RADIUS or TACACS+ authentication server
- DHCP snooping events
- ARP protection events

In addition, you can enable the switch to send the following types of notifications to configured trap receivers. For information on how to configure each notification, refer to the ProCurve software guide under which the notification is listed.

- *Management and Configuration Guide:*
 - Configuration changes
 - ICMP rate-limiting
 - Instrumentation monitoring
 - Link-Layer Discovery Protocol (LLDP)
 - Ping tests
 - Power over Ethernet (POE): port toggle, power limit
 - RMON

- *Advance Traffic Management Guide:*
 - Loop protection
 - Spanning Tree (STP, RSTP, MSTP)
- *Access Security Guide:*
 - MAC lockdown
 - MAC lockout
 - Uni-Directional Link Detection (UDLD)
 - Virus throttling
- *Multicast and Routing Guide:*
 - OSPF
 - PIM
 - Virtual Router Redundancy Protocol (VRRP)

General Steps for Configuring SNMP Notifications

To configure SNMP notifications, follow these general steps:

1. Determine the versions of SNMP notifications that you want to use in your network.

If you want to use SNMPv1 and SNMPv2c traps, you must also configure a trap receiver. Refer to the following sections and follow the required configuration procedures:

- “SNMPv1 and SNMPv2c Traps” on page 14-19
- “Configuring an SNMP Trap Receiver” on page 14-19
- “Enabling SNMPv2c Informs” on page 14-21

If you want to use SNMPv3 notifications (including traps), you must also configure an SNMPv3 management station. Follow the required configuration procedure in the following section:

- “Configuring SNMPv3 Notifications” on page 14-23

2. To reconfigure any of the SNMP notifications that are enabled by default to be sent to a management station (trap receiver), refer to these sections:

-

- “Enabling Link-Change Traps” on page 14-28

3. (Optional) Refer to the following sections to configure optional SNMP notification features and verify the current configuration:

- “Configuring the Source IP Address for SNMP Notifications” on page 14-29
- “Displaying SNMP Notification Configuration” on page 14-31

SNMPv1 and SNMPv2c Traps

The switches covered in this guide support the following functionality from earlier SNMP versions (SNMPv1 and SNMPv2c):

- **Trap receivers:** A *trap receiver* is a management station to which the switch sends SNMP traps and (optionally) event log messages sent from the switch. From the CLI you can configure up to ten SNMP trap receivers to receive SNMP traps from the switch.
- **Fixed or “Well-Known” Traps:** A switch automatically sends fixed traps (such as “coldStart”, “warmStart”, “linkDown”, and “linkUp”) to trap receivers using the **public** community name. These traps cannot be redirected to other communities. If you change or delete the default **public** community name, these traps are not sent.
- **Thresholds:** A switch automatically sends all messages created when a system threshold is reached to the network management station that configured the threshold, regardless of the trap receiver configuration.

Configuring an SNMP Trap Receiver

Use the **snmp-server host** command to configure a trap receiver that can receive SNMPv1 and SNMPv2c traps, and (optionally) event log messages. When you configure a trap receiver, you specify its community membership, management station IP address, and (optionally) the type of event log messages to be sent.

If you specify a community name that does not exist—that is, has not yet been configured on the switch—the switch still accepts the trap receiver assignment. However, no traps will be sent to that trap receiver until the community to which it belongs has been configured on the switch.

Syntax: snmp-server host <ipv4-addr | ipv6-addr> <community name>

*Configures a destination network management station to receive SNMPv1/v2c traps, and (optionally) event log messages sent as traps from the switch, using the specified community name and destination IPv4 or IPv6 address. You can specify up to ten trap receivers (network management stations). The default community name is **public**.*

[<none | all | non-info | critical | debug>]

(Optional) Configures the security level of the event log messages you want to send as traps to a trap receiver (see table 14-1, “Security Levels for Event Log Messages Sent as Traps”).

- *The type of event log message that you specify applies only to event log messages, not to threshold traps.*
- *For each configured event level, the switch continues to send threshold traps to all network management stations that have the appropriate threshold level configured.*
- *If you do not specify an event level, the switch uses the default value (**none**) and sends no event log messages as traps.*

[<inform>]

(Optional) Configures the switch to send SNMPv2 inform requests when certain events occur. See “Enabling SNMPv2c Informs” on page 14-21 for more information.

Table 14-1. Security Levels for Event Log Messages Sent as Traps

Security Level	Action
None (default)	Sends no event log messages.
All	Sends all event log messages.
Non-Info	Sends all event log messages that are not for information only.
Critical	Sends only event log messages for critical error conditions.
Debug	Sends only event log messages needed to troubleshoot network- and switch-level problems.

For example, to configure a trap receiver in a community named "red-team" with an IP address of 10.28.227.130 to receive only "critical" event log messages, you can enter the following command:

```
ProCurve (config) # snmp-server host 10.28.227.130 red-team  
critical
```

Notes

To replace one community name with another for the same IP address, you must first enter the **no snmp-server host** <community-name> <ipv4-address|ipv6-address> command to delete the unwanted community name. Otherwise, if you add a new community name with an IP address that is already used with a different community name, two valid community name entries are created for the same management station.

If you do not specify the event level ([<none|all|non-info|critical|debug>]), the switch does not send event log messages as traps. However, "well-known" traps and threshold traps (if configured) are still sent.

Enabling SNMPv2c Informs

On a switch enabled for SNMPv2c, you can use the **snmp-server host inform** command to send inform requests when certain events occur. When an SNMP Manager receives an inform request, it can send an SNMP response back to the sending agent on the switch to let the agent know that the inform request reached its destination.

If the sending agent on the switch does not receive an SNMP response back from the SNMP Manager within the timeout period, the inform request may be resent, based on the retry count value.

When you enable SNMPv2c inform requests to be sent, you must specify the IP address and community name of the management station that will receive the inform notification.

Syntax: [no] snmp-server host <ipv4-addr|ipv6-addr> <community name>
inform [retries <count>] [timeout <interval>]]

*Enables (or disables) the **inform** option for SNMPv2c on the switch and allows you to configure options for sending SNMP inform requests.*

retries: *Maximum number of times to resend an inform request if no SNMP response is received. Default: 3*

timeout: *Number of seconds to wait for an acknowledgement before resending the inform request. Default: 15 seconds*

Note

The **retries** and **timeout** values are not used to send trap requests.

To verify the configuration of SNMPv2c informs, enter the **show snmp-server** command:

```
ProCurve Switch 5406zl(config)# show snmp-server
SNMP Communities
Community Name      MIB View Write Access
-----
public              Manager  Unrestricted

Trap Receivers
Link-Change Traps Enabled on Ports [All] : All
...

Address              Community      Events Sent  Notify Type  Retry  Timeout
-----
15.28.333.456       guest          All          inform        3      15

Excluded MIBs
Snmp Response Pdu Source-IP Information
Selection Policy    : Default rfc1517

Trap Pdu Source-IP Information
Selection Policy    : Configured IP
Ip Address          : 10.10.10.10
```

SNMPv2c Inform configuration

Figure 14-8. Display of SNMPv2c Inform Configuration

Configuring SNMPv3 Notifications

The SNMPv3 notification process allows messages that are passed via SNMP between the switch and a network management station to be authenticated and encrypted.

To configure SNMPv3 notifications, follow these steps:

1. Enable SNMPv3 operation on the switch by entering the **snmpv3 enable** command (see “SNMP Version 3 Commands” on page 14-6).

When SNMPv3 is enabled, the switch supports:

- Reception of SNMPv3 notification messages (traps and informs)
 - Configuration of initial users
 - (Optional) Restriction of non-SNMPv3 messages to “read only”
2. Configure SNMPv3 users by entering the **snmpv3 user** command (see “SNMPv3 Users” on page 14-7). Each SNMPv3 user configuration is entered in the User Table.
 3. Assign SNMPv3 users to security groups according to their level of access privilege by entering the **snmpv3 group** command (see “Assigning Users to Groups” on page 14-10).
 4. Define the name of an SNMPv3 notification configuration by entering the **snmpv3 notify** command.

Syntax: [no] snmpv3 notify <notify_name> tagvalue <tag_name>

*Associates the name of an SNMPv3 notification configuration with a tag name used (internally) in SNMPv3 commands. To delete a notification-to-tag mapping, enter **no snmpv3 notify <notify_name>**.*

notify < notify_name >

Specifies the name of an SNMPv3 notification configuration.

tagvalue < tag_name >

*Specifies the name of a tag value used in other SNMPv3 commands, such as **snmpv3 targetaddress params taglist <tag_name>** in Step 5.*

5. Configure the target address of the SNMPv3 management station to which SNMPv3 informs and traps are sent by entering the **snmpv3 targetaddress** command.

Syntax: [no] snmpv3 targetaddress < ipv4-addr | ipv6-addr > < name >

Configures the IPv4 or IPv6 address, name, and configuration filename of the SNMPv3 management station to which notification messages are sent.

params < params_name >

*Name of the SNMPv3 station's parameters file. The parameters filename configured with **params** <params_name> must match the **params** <params_name> value entered with the **snmpv3 params** command in Step 6.*

taglist <tag_name> [tag_name] ...

Specifies the SNMPv3 notifications (identified by one or more <tag_name> values) to be sent to the IP address of the SNMPv3 management station.

*You can enter more than one <tag_name> value. Each <tag_name> value must be already associated with the name of an SNMPv3 notification configuration entered with the **snmpv3 notify** command in Step 4.*

Use a blank space to separate <tag_name> values.

*You can enter up to 103 characters in <tag_name> entries following the **taglist** keyword.*

[filter < none | debug | all | not-info | critical >]

*(Optional) Configures the type of messages sent to a management station. Default: **none**.*

[udp-port < port >]

*(Optional) Specifies the UDP port to use. Default: **162**.*

[port-mask < mask >]

*(Optional) Specifies a range of UDP ports. Default: **0**.*

[addr-mask < mask >]

*(Optional) Specifies a range of IP addresses as destinations for notification messages. Default: **0**.*

[retries < value >]

*(Optional) Number of times a notification is retransmitted if no response is received. Range: 1-255. Default: **3**.*

Syntax: [no] snmpv3 targetaddress < ipv4-addr | ipv6-addr > < name >
—Continued—

[timeout < value >]

*(Optional) Time (in millisecond increments) allowed to receive a response from the target before notification packets are retransmitted. Range: 0-2147483647. Default: **1500** (15 seconds).*

[max-msg-size < size >]

*(Optional) Maximum number of bytes supported in a notification message to the specified target. Default: **1472***

6. Create a configuration record for the target address with the **snmpv3 params** command.

Syntax [no] snmpv3 params < params_name > user < user_name >

*Applies the configuration parameters and IP address of an SNMPv3 management station (from the **params** < params_name > value configured with the **snmpv3 targetaddress** command in Step 5) to a specified SNMPv3 user (from the **user** < user_name > value configured with the **snmpv3 user** command in Step 2).*

*If you enter the **snmpv3 params user** command, you must also configure a security model (**sec-model**) and message processing algorithm (**msg-processing**).*

< sec-model < ver1 | ver2c | ver3 >

*Configures the security model used for SNMPv3 notification messages sent to the management station configured with the **snmpv3 targetaddress** command in Step 5.*

*If you configure the security model as **ver3**, you must also configure the message processing value as **ver3**.*

< msg-processing < ver1 | ver2c | ver3 > [noauth | auth | priv]

Configures the algorithm used to process messages sent to the SNMPv3 target address.

*If you configure the message processing value as **ver3** and the security model as **ver3**, you must also configure a security services level (**noauth**, **auth**, or **priv**).*

An example of how to configure SNMPv3 notification is shown here:

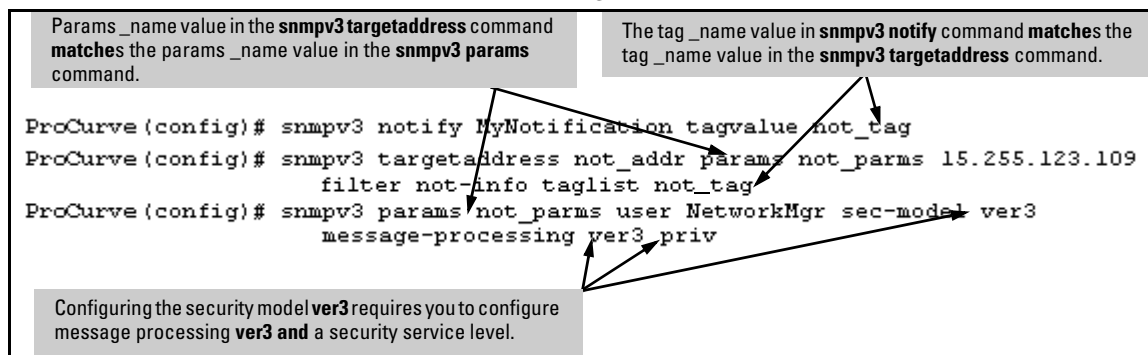


Figure 14-9. Example of an SNMPv3 Notification Configuration

Managing Network Security Notifications

By default, a switch is enabled to send the SNMP notifications listed in “Supported Notifications” on page 14-17 when a network security event (for example, authentication failure) occurs. However, before security notifications can be sent, you must first configure one or more trap receivers or SNMPv3 management stations as described in:

- “Configuring an SNMP Trap Receiver” on page 14-19
- “Configuring SNMPv3 Notifications” on page 14-23

You can manage the default configuration of the switch to disable and re-enable notifications to be sent for the following types of security events:

- SNMP authentication failure
- Port-security (web, MAC, or 802.1X) authentication failure
- Invalid password entered in a login attempt through a direct serial, Telnet, or SSH connection
- Unable to establish a connection with the RADIUS or TACACS+ authentication server
- DHCP snooping events
- ARP protection events
- Manager password changes

To enable or disable notification/traps for network security failures and other security events, enter the **snmp-server enable traps** command.

Syntax: [no] snmp-server enable traps [snmp-auth | password-change-mgr | login-failure-mgr | port-security | auth-server-fail | dhcp-snooping | arp-protect]

Enables or disables sending one of the following types of security notification to configured trap receivers:

- **snmp-auth** sends a trap for a failed authentication attempt via SNMP.
- **password-change-mgr** sends a trap when a manager password is reset.
- **login-failure-mgr** sends a trap for a failed login with a manager password.
- **port-security** sends a trap for a failed authentication attempt through a web, MAC, or 801.X authentication session.
- **auth-server-fail** sends a trap if the connection with a RADIUS or TACACS+ authentication server fails.
- **dhcp-snooping** sends a trap if DHCP packets are received from an untrusted source or if DHCP packets contain an invalid IP-to-MAC binding.
- **arp-protect** sends a trap if ARP packets are received with an invalid source or destination MAC address, an invalid IP address, or an invalid IP-to-MAC binding.

To determine the specific cause of a security event, check the event log in the console interface to see why a trap was sent. For more information, refer to “Using the Event Log for Troubleshooting Switch Problems” on page C-27.

To display the current configuration for network security notifications, enter the **show snmp-server traps** command. Note that command output is a subset of the information displayed with the **show snmp-server** command in Figure 14-12.

```
ProCurve(config)# show snmp-server traps

Trap Receivers

Link-Change Traps Enabled on Ports [All] : A1-A24

Trap Category                               Current Trap Configuration
-----
SNMP Authentication                         extended
Password change                             enabled
Login failures                              enabled
Port-Security                              enabled
Authorization Server Contact                enabled
ARP Protection                              enabled
DHCP Snooping                              enabled

Address      Community  Events Sent  Notify Type  Retry  Timeout
-----
15.255.5.225  user1      All         trap         3      15

Excluded MIBs
```

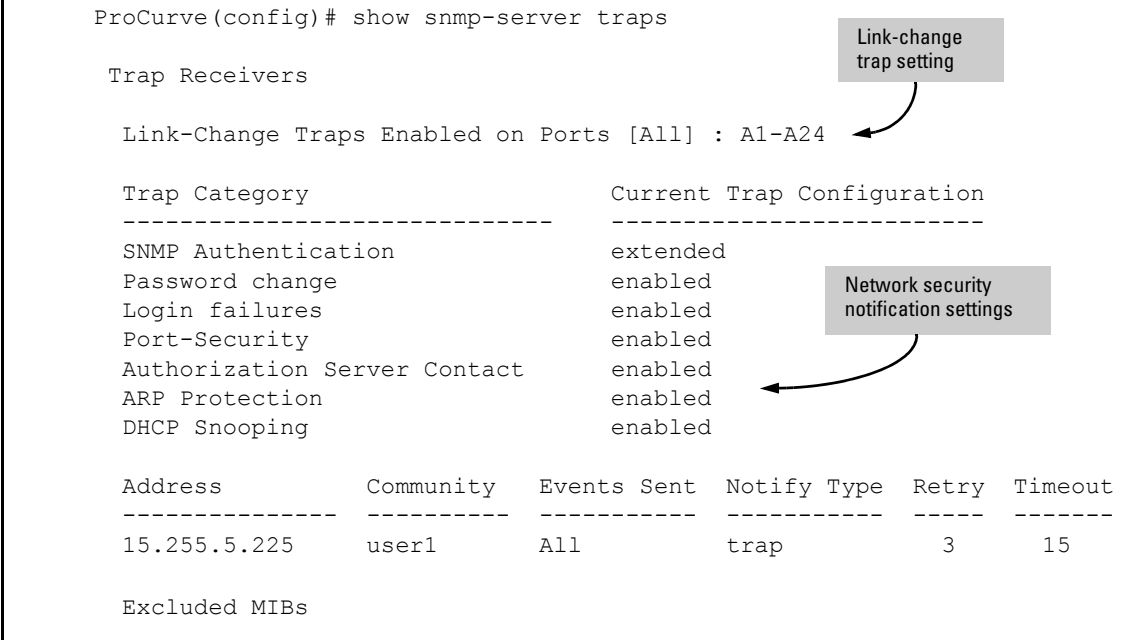


Figure 14-10. Display of Configured Network Security Notifications

Enabling Link-Change Traps

By default a switch is enabled to send a trap when the link state on a port changes from up to down (linkDown) or down to up (linkUp). To reconfigure the switch to send link-change traps to configured trap receivers, enter the **snmp-server enable traps link-change** command.

Syntax: [no] snmp-server enable traps link-change<port-list> [all]

Enables or disables the switch to send a link-change trap to configured trap receivers when the link state on a port goes from up to down or down to up.

*Enter **all** to enable or disable link-change traps on all ports on the switch.*

Configuring the Source IP Address for SNMP Notifications

The switch uses an interface IP address as the source IP address in IP headers when sending SNMP notifications (traps and informs) or responses to SNMP requests.

For multi-netted interfaces, the source IP address is the IP address of the outbound interface of the SNMP reply, which may differ from the destination IP address in the IP header of the received request. For security reasons, it may be desirable to send an SNMP reply with the IP address of the destination interface (or a specified IP address) on which the corresponding SNMP request was received.

To configure the switch to use the source IP address on which an SNMP request was received in SNMP notification/traps and replies, enter the **snmp-server response-source** and **snmp-server trap-source** commands.

Syntax: [no] snmp-server response-source [dst-ip-of-request | <ipv4-addr | ipv6-addr> | loopback<0-7>]

Specifies the source IP address of the SNMP response PDU. The default SNMP response PDU uses the IP address of the active interface from which the SNMP response was sent as the source IP address.

*The **no** form of the command resets the switch to the default behavior (compliant with rfc-1517).*

Default: Interface IP address

dst-ip-of-request: *Destination IP address of the SNMP request PDU that is used as the source IP address in an SNMP response PDU.*

<ipv4-addr | ipv6-addr>: *User-defined interface IP address that is used as the source IP address in an SNMP response PDU. Both IPv4 and IPv6 addresses are supported.*

loopback <0-7>: *IP address configured for the specified loopback interface that is used as the source IP address in an SNMP response PDU. If multiple loopback IP addresses are configured, the lowest alphanumeric address is used.*

For example, to use the IP address of the destination interface on which an SNMP request was received as the source IP address in the IP header of SNMP traps and replies, enter the following command:

```
ProCurve(config)# snmp-server response-source  
dst-ip-of-request
```

To configure the switch to use a specified source IP address in generated trap PDUs, enter the **snmp-server trap-source** command.

Syntax: [no] snmp-server trap-source [<ipv4-addr> | loopback<0-7>]

*Specifies the source IP address to be used for a trap PDU. The **no** form of the command resets the switch to the default behavior (compliant with rfc-1517).
Default: Use the interface IP address in generated trap PDUs.
<ipv4-addr>: User-defined interface IPv4 address that is used as the source IP address in generated traps. IPv6 addresses are not supported.*

loopback <0-7>: IP address configured for the specified loopback interface that is used as the source IP address in a generated trap PDU. If multiple loopback IP addresses are configured, the lowest alphanumeric address is used.

Notes

When you use the **snmp-server response-source** and **snmp-server trap-source** commands, note the following behavior:

- The **snmp-server response-source** and **snmp-server trap-source** commands configure the source IP address for IPv4 interfaces only.
- You must manually configure the **snmp-server response-source** value if you wish to change the default user-defined interface IP address that is used as the source IP address in SNMP traps (RFC 1517).
- The values configured with the **snmp-server response-source** and **snmp-server trap-source** commands are applied globally to all interfaces that are sending SNMP responses or SNMP trap PDUs.
- Only the source IP address field in the IP header of the SNMP response PDU can be changed.
- Only the source IP address field in the IP header and the SNMPv1 Agent Address field of the SNMP trap PDU can be changed.

To verify the configuration of the interface IP address used as the source IP address in IP headers for SNMP replies and traps sent from the switch, enter the **show snmp-server** command to display the SNMP policy configuration.

```
ProCurve_8212(config)# show snmp-server

SNMP Communities

Community Name   MIB View Write Access
-----
public          Manager  Unrestricted

Trap Receivers
Link-Change Traps Enabled on Ports [All] : All

...

Excluded MIBs
Snm Response Pdu Source-IP Information
Selection Policy : dstIpOfRequest

Trap Pdu Source-IP Information
Selection Policy : Configured IP
Ip Address      : 10.10.10.10
```

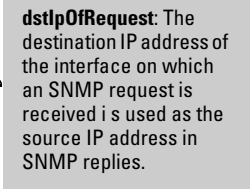


Figure 14-11. Display of Source IP Address Configuration

Displaying SNMP Notification Configuration

Use the **show snmp-server** command to display the currently configured:

- Management stations (trap receivers)
- Settings for network security notifications and link-change traps
- SNMP communities

Syntax: show snmp-server

Displays the currently configured notification settings for versions SNMPv1 and SNMPv2c traps, including SNMP communities, trap receivers, link-change traps, and network security notifications.

In the following example, the **show snmp-server** command output shows that the switch has been configured to send SNMP traps and notifications to management stations that belong to the “public”, “red-team”, and “blue-team” communities.

```
ProCurve(config)# show snmp-server

SNMP Communities
Community Name  MIB View Write Access
-----
public          Operator Restricted
blue-team      Manager Unrestricted
red-team       Manager Unrestricted

Trap Receivers

Link-Change Traps Enabled on Ports [All] : All

Trap Category          Current Trap Configuration
-----
SNMP Authentication   extended
Password change       enabled
Login failures        enabled
Port-Security         enabled
Authorization Server Contact enabled
ARP Protection        enabled
DHCP Snooping        enabled

Address      Community  Events Sent  Notify Type  Retry  Timeout
-----
10.28.227.200 public     All          trap         3      15
10.28.227.105 red-team   Critical     trap         3      15
10.28.227.120 blue-team  Not-INFO     trap         3      15
...
```

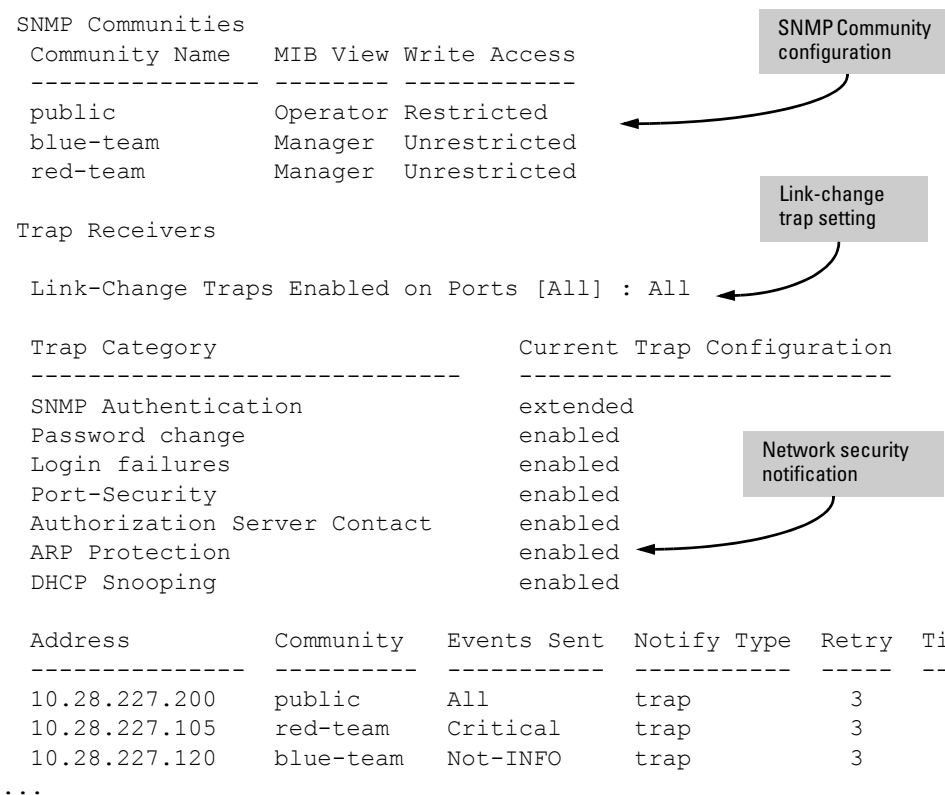


Figure 14-12. Display of SNMP Notification Configuration

Advanced Management: RMON

The switch supports RMON (Remote Monitoring) on all connected network segments. This allows for troubleshooting and optimizing your network.

The following RMON groups are supported:

- Ethernet Statistics (except the numbers of packets of different frame sizes)
- Alarm
- History (of the supported Ethernet statistics)
- Event

The RMON agent automatically runs in the switch. Use the RMON management station on your network to enable or disable specific RMON traps and events. Note that you can access the Ethernet statistics, Alarm, and Event groups from the ProCurve Manager network management software. For more on ProCurve Manager, visit the ProCurve Networking web site at

www.procurve.com

Click on **products index**, then look for the ProCurve Manager topic under the **Network Manager** bar.

CLI-Configured sFlow with Multiple Instances

In earlier software releases, sFlow was configured on the switch via SNMP using a single sFlow instance. Beginning with software release K.11.34, sFlow can also be configured via the CLI for up to three distinct sFlow instances: once enabled, an sFlow receiver/destination can be independently configured for full flow-sampling and counter-polling. CLI-configured sFlow instances may be saved to the startup configuration to persist across a switch reboot.

Terminology

sFlow — An industry standard sampling technology, defined by RFC 3176, used to continuously monitor traffic flows on all ports providing network-wide visibility into the use of the network.

sFlow agent — A software process that runs as part of the network management software within a device. The agent packages data into datagrams that are forwarded to a central data collector.

sFlow destination — The central data collector that gathers datagrams from sFlow-enabled switch ports on the network. The data collector decodes the packet headers and other information to present detailed Layer 2 to Layer 7 usage statistics.

Configuring sFlow

The following sFlow commands allow you to configure sFlow instances via the CLI.

Syntax: [no] sflow <receiver-instance> destination <ip-address> [udp-port-num]

Enables an sFlow receiver/destination. The receiver-instance number must be a 1, 2, or 3. By default, the udp destination port number is 6343.

To disable an sFlow receiver/destination, enter no sflow <receiver-instance>.

Syntax: sflow <receiver-instance> sampling <port-list> <sampling rate>

Once an sFlow receiver/destination has been enabled, this command enables flow sampling for that instance. The receiver-instance number is 1, 2, or 3, and the sampling rate is the allowable non-zero skipcount for the specified port or ports.

To disable flow-sampling for the specified port-list, repeat the above command with a sampling rate of "0".

Syntax: sflow <receiver-instance> polling <port-list> <polling interval>

Once an sFlow receiver/destination has been enabled, this command enables counter polling for that instance. The receiver-instance number is 1, 2, or 3, and the polling interval may be set to an allowable non-zero value to enable polling on the specified port or ports.

To disable counter-polling for the specified port-list, repeat the above command with a polling interval of "0".

Note

Under the multiple instance implementation, sFlow can be configured via the CLI or via SNMP. However, CLI-owned sFlow configurations cannot be modified via SNMP, whereas SNMP-owned instances can be disabled via the CLI using the **no sflow <receiver-instance>** command.

Viewing sFlow Configuration and Status

The following sFlow commands allow you to display sFlow configuration and status via the CLI.

Syntax: show sflow agent

Displays sFlow agent information. The agent address is normally the ip address of the first vlan configured.

Syntax: show sflow <receiver instance> destination

Displays information about the management station to which the sFlow sampling-polling data is sent.

Syntax: show sflow <receiver instance> sampling-polling <port-list/range>

Displays status information about sFlow sampling and polling.

The **show sflow agent** command displays read-only switch agent information. The version information shows the sFlow version, MIB support and software versions; the agent address is typically the ip address of the first vlan configured on the switch.

```
ProCurve# show sflow agent

Version          1.3;HP;K.11.40
Agent Address    10.0.10.228
```

Figure 14-13. Example of Viewing sFlow Agent Information

The **show sflow <instance> destination** command includes information about the management-station's destination address, receiver port, and owner.

```
ProCurve# show sflow 2 destination

Destination Instance      2
sflow                     Enabled
Datagrams Sent           221
Destination Address       10.0.10.41
Receiver Port             6343
Owner                    Administrator, CLI-owned, Instance 2
Timeout (seconds)        99995530
Max Datagram Size        1400
Datagram Version Support  5
```

Figure 14-14. Example of Viewing sFlow Destination Information

Note the following details:

- **Destination Address** remains blank unless it has been configured.
- **Datagrams Sent** shows the number of datagrams sent by the switch agent to the management station since the switch agent was last enabled.
- **Timeout** displays the number of seconds remaining before the switch agent will automatically disable sFlow (this is set by the management station and decrements with time).
- **Max Datagram Size** shows the currently set value (typically a default value, but this can also be set by the management station).

The **show sflow <instance> sampling-polling** [port-list] command displays information about sFlow sampling and polling on the switch. You can specify a list or range of ports for which to view sampling information.

```
ProCurve# show sflow 2 sampling-polling A1-A4
```

Number denotes the sampling/polling instance to which the receiver is coupled.

Port	Sampling		Dropped				Polling							
	Enabled	Rate	Header	Samples				Enabled	Interval					
A1	Yes (2)	40	128	1	2	3	4	5	6	7	8	9	0	---
A2	---	---	---	0				Yes (1)	60					
A3	No (1)	0	100	898703				No	30					
A4	Yes (3)	50	128	0				No (3)	0					

Figure 14-15. Example of Viewing sFlow Sampling and Polling Information

Note

The sampling and polling instances (noted in parentheses) coupled to a specific receiver instance are assigned dynamically, and so the instance numbers may not always match. The key thing to note is whether sampling or polling is enabled on a port, and the sampling rates or polling intervals for the receiver instance configured on each port.

LLDP (Link-Layer Discovery Protocol)

To standardize device discovery on all ProCurve switches, LLDP will be implemented while offering limited read-only support for CDP as documented in this manual. For the latest information on your switch model, consult the Release Notes (available on the ProCurve Networking web site). If LLDP has not yet been implemented (or if you are running an older version of software), consult a previous version of the Management and Configuration Guide for device discovery details.

Table 14-2. LLDP and LLDP-MED Features

Feature	Default	Menu	CLI	Web
View the switch's LLDP configuration	n/a	—	page 14-45	—
Enable or disable LLDP on the switch	Enabled	—	page 14-41	—
Change the transmit interval (refresh-interval) for LLDP packets	30 seconds	—	page 14-48	—
Change the holdtime multiplier for LLDP Packets (holdtime-multiplier x refresh-interval = time-to-live)	4 seconds	—	page 14-41	—
Change the delay interval between advertisements	2 seconds	—	page 14-49	—
Changing the reinitialization delay interval	2 seconds	—	page 14-50	—
Configuring SNMP notification support	Disabled	—	page 14-51	—
Configuring transmit and receive modes	tx_rx	—	page 14-52	—
Configuring basic LLDP per-port advertisement content	Enabled	—	page 14-53	—
Configuring port speed and duplex advertisements for optional LLDP and mandatory LLDP-MED applications	Enabled	—	page 14-73	—
Configuring topology change notification for LLDP-MED	Enable	—	page 14-59	—
Changing the fast-start duration for LLDP-MED	5 sec	—	page 14-61	—
Configuring LLDP-MED Advertising	Enabled	—	page 14-53	—
Configuring LLDP-MED device location data	None	—	page 14-71	—
Displaying Advertisement Data and Statistics	n/a	—	page 14-75	—

LLDP (Link Layer Discovery Protocol): provides a standards-based method for enabling the switches covered in this guide to advertise themselves to adjacent devices and to learn about adjacent LLDP devices.

LLDP-MED (LLDP Media Endpoint Discovery): Provides an extension to LLDP and is designed to support VoIP deployments.

Note

LLDP-MED is an extension for LLDP, and the switch requires that LLDP be enabled as a prerequisite to LLDP-MED operation.

An SNMP utility can progressively discover LLDP devices in a network by:

1. Reading a given device's Neighbors table (in the Management Information Base, or MIB) to learn about other, neighboring LLDP devices.
2. Using the information learned in step 1 to find and read the neighbor devices' Neighbors tables to learn about additional devices, and so on.

Also, by using **show** commands to access the switch's neighbor database for information collected by an individual switch, system administrators can learn about other devices connected to the switch, including device type (capability) and some configuration information. In VoIP deployments using LLDP-MED on the switches covered in this guide, additional support unique to VoIP applications is also available. Refer to "LLDP-MED (Media-Endpoint-Discovery)" on page 14-56.

Terminology

Adjacent Device: Refer to "Neighbor or Neighbor Device".

Advertisement: See LLDPDU.

Active Port: A port linked to another active device (regardless of whether MSTP is blocking the link).

ELIN (Emergency Location Identification Number): A valid telephone number in the North American Numbering Plan format and assigned to a multiline telephone system operator by the appropriate authority. This number calls a public service answering point (PSAP) and relays automatic location identification data to the PSAP.

LLDP: Link Layer Discovery Protocol:

- Switches covered in this guide: IEEE 802.1AB

LLDP-Aware: A device that has LLDP in its operating code, regardless of whether LLDP is enabled or disabled.

LLDP Device: A switch, server, router, or other device running LLDP.

LLDP Neighbor: An LLDP device that is either directly connected to another LLDP device or connected to that device by another, non-LLDP Layer 2 device (such as a hub) Note that an 802.1D-compliant switch does not forward LLDP data packets even if it is not LLDP-aware.

LLDPDU (LLDP Data Unit): LLDP data packet are transmitted on active links and include multiple TLVs containing global and per-port switch information. In this guide, LLDPDUs are termed “advertisements” or “packets”.

LLDP-MED (Link Layer Discover Protocol Media Endpoint Discovery): The TIA telecommunications standard produced by engineering subcommittee TR41.4, “VoIP Systems — IP Telephony infrastructure and Endpoints” to address needs related to deploying VoIP equipment in IEEE 802-based environments. This standard will be published as ANSI/TIA-1057.

MIB (Management Information Base): An internal database the switch maintains for configuration and performance information.

MLTS (Multiline Telephone System): A network-based and/or premises-based telephone system having a common interface with the public switched telephone system and having multiple telephone lines, common control units, multiple telephone sets, and control hardware and software.

NANP (North American Numbering Plan): A ten-digit telephone number format where the first three digits are an area code and the last seven-digits are a local telephone number.

Neighbor: See “LLDP Neighbor”.

Non-LLDP Device: A device that is not capable of LLDP operation.

PD (Powered Device): This is an IEEE 802.3af-compliant device that receives its power through a direct connection to a 10/100Base-TX PoE RJ-45 port in a ProCurve fixed-port or chassis-based switch. Examples of PDs include Voice-over-IP (VoIP) telephones, wireless access points, and remote video cameras.

PSAP (Public Safety Answering Point): PSAPs are typically emergency telephone facilities established as a first point to receive emergency (911) calls and to dispatch emergency response services such as police, fire and emergency medical services.

PSE (Power-Sourcing Equipment): A PSE, such as a PoE module installed in a switch covered in this guide, provides power to IEEE 802.3af-compliant PDs directly connected to the ports on the module.

TLV (Type-Length-Value): A data unit that includes a data type field, a data unit length field (in bytes), and a field containing the actual data the unit is designed to carry (as an alphanumeric string, a bitmap, or a subgroup of information). Some TLVs include subelements that occur as separate data points in displays of information maintained by the switch for LLDP advertisements. (That is, some TLVs include multiple data points or subelements.)

General LLDP Operation

An LLDP packet contains data about the transmitting switch and port. The switch advertises itself to adjacent (neighbor) devices by transmitting LLDP data packets out all ports on which outbound LLDP is enabled, and reading LLDP advertisements from neighbor devices on ports that are inbound LLDP-enabled. (LLDP is a one-way protocol and does not include any acknowledgement mechanism.) An LLDP-enabled port receiving LLDP packets inbound from neighbor devices stores the packet data in a Neighbor database (MIB).

LLDP-MED

This capability is an extension to LLDP and is available on the switches covered in this guide. Refer to “LLDP-MED (Media-Endpoint-Discovery)” on page 14-56.

Packet Boundaries in a Network Topology

- Where multiple LLDP devices are directly connected, an outbound LLDP packet travels only to the next LLDP device. An LLDP-capable device does not forward LLDP packets to any other devices, regardless of whether they are LLDP-enabled.
- An intervening hub or repeater forwards the LLDP packets it receives in the same manner as any other multicast packets it receives. Thus, two LLDP switches joined by a hub or repeater handle LLDP traffic in the same way that they would if directly connected.
- Any intervening 802.1D device or Layer-3 device that is either LLDP-unaware or has disabled LLDP operation drops the packet.

Configuration Options

Enable or Disable LLDP on the Switch. In the default configuration, LLDP is globally enabled on the switch. To prevent transmission or receipt of LLDP traffic, you can disable LLDP operation (page 14-41)

Enable or Disable LLDP-MED. In the default configuration for the switches covered in this guide, LLDP-MED is enabled by default. (Requires that LLDP is also enabled.) For more information, refer to “LLDP-MED (Media-Endpoint-Discovery)” on page 14-56.

Change the Frequency of LLDP Packet Transmission to Neighbor Devices. On a global basis, you can increase or decrease the frequency of outbound LLDP advertisements (page 14-41).

Change the Time-To-Live for LLDP Packets Sent to Neighbors. On a global basis, you can increase or decrease the time that the information in an LLDP packet outbound from the switch will be maintained in a neighbor LLDP device (page 14-41).

Transmit and Receive Mode. With LLDP enabled, the switch periodically transmits an LLDP advertisement (packet) out each active port enabled for outbound LLDP transmissions, and receives LLDP advertisements on each active port enabled to receive LLDP traffic (page 14-52). Per-Port configuration options include four modes:

- **Transmit and Receive (tx_rx):** This is the default setting on all ports. It enables a given port to both transmit and receive LLDP packets, and to store the data from received (inbound) LLDP packets in the switch’s MIB.
- **Transmit only (txonly):** This setting enables a port to transmit LLDP packets that can be read by LLDP neighbors. However, the port drops inbound LLDP packets from LLDP neighbors without reading them. This prevents the switch from learning about LLDP neighbors on that port.
- **Receive only (rxonly):** This setting enables a port to receive and read LLDP packets from LLDP neighbors, and to store the packet data in the switch’s MIB. However, the port does not transmit outbound LLDP packets. This prevents LLDP neighbors from learning about the switch through that port.
- **Disable (disable):** This setting disables LLDP packet transmissions and reception on a port. In this state, the switch does not use the port for either learning about LLDP neighbors or informing LLDP neighbors of its presence.

SNMP Notification. You can enable the switch to send a notification to any configured SNMP trap receiver(s) when the switch detects a remote LLDP data change on an LLDP-enabled port (page 14-51).

Per-Port (Outbound) Data Options. The following table lists the information the switch can include in the per-port, outbound LLDP packets it generates. In the default configuration, all outbound LLDP packets include this information in the TLVs transmitted to neighbor devices. However, you can configure LLDP advertisements on a per-port basis to omit some of this information (page 14-53).

Table 14-3. Data Available for Basic LLDP Advertisements

Data Type	Configuration Options	Default	Description
Time-to-Live	See note 1.	120 Seconds	The length of time an LLDP neighbor retains the advertised data before discarding it.
Chassis Type ^{2, 6}	N/A	Always Enabled	Indicates the type of identifier used for Chassis ID.
Chassis ID ⁶	N/A	Always Enabled	Uses base MAC address of the switch.
Port Type ^{3, 6}	N/A	Always Enabled	Uses "Local", meaning assigned locally by LLDP.
Port Id ⁶	N/A	Always Enabled	Uses port number of the physical port. In the switches covered in this guide, this is an internal number reflecting the reserved slot/port position in the chassis. For more information on this numbering scheme, refer to figures D-2 and D-3 in Appendix D, "MAC Address Management" of the <i>Management and Configuration Guide</i> for your switch.
Remote Management Address			
Type ^{4, 6}	N/A	Always Enabled	Shows the network address type.
Address ⁴	Default or Configured	Uses a default address selection method unless an optional address is configured. See "Remote Management Address" on page 14-43.	
System Name ⁶	Enable/Disable	Enabled	Uses the switch's assigned name.
System Description ⁶	Enable/Disable	Enabled	Includes switch model name and running software version, and ROM version.
Port Description ⁶	Enable/Disable	Enabled	Uses the physical port identifier.
System capabilities supported ^{5, 6}	Enable/Disable	Enabled	Identifies the switch's primary capabilities (bridge, router).
System capabilities enabled ^{5, 6}	Enable/Disable	Enabled	Identifies the primary switch functions that are enabled, such as routing.

Data Type	Configuration Options	Default	Description
¹			The Packet Time-to-Live value is included in LLDP data packets. (Refer to “Changing the Time-to-Live for Transmitted Advertisements” on page 14-49.)
²			Subelement of the Chassis ID TLV.
³			Subelement of the Port ID TLV.
⁴			Subelement of the Remote-Management-Address TLV.
⁵			Subelement of the System Capability TLV.
⁶			Populated with data captured internally by the switch. For more on these data types, refer to the IEEE P802.1AB Standard.

Remote Management Address. The switch always includes an IP address in its LLDP advertisements. This can be either an address selected by a default process, or an address configured for inclusion in advertisements. Refer to “IP Address Advertisements” on page 14-44.

Debug Logging. You can enable LLDP debug logging to a configured debug destination (Syslog server and/or a terminal device) by executing the **debug lldp** command. (For more on Debug and Syslog, refer to the “Troubleshooting” appendix in this guide.) Note that the switch’s Event Log does not record usual LLDP update messages.

Options for Reading LLDP Information Collected by the Switch

You can extract LLDP information from the switch to identify adjacent LLDP devices. Options include:

- Using the switch’s **show lldp info** command options to display data collected on adjacent LLDP devices—as well as the local data the switch is transmitting to adjacent LLDP devices (page 14-45).
- Using an SNMP application that is designed to query the Neighbors MIB for LLDP data to use in device discovery and topology mapping. 3400/6400 only?
- Using the **walkmib** command to display a listing of the LLDP MIB objects

LLDP and LLDP-MED Standards Compatibility

The operation covered by this section is compatible with these standards:

- IEEE P802.1AB
- RFC 2922 (PTOPO, or Physical Topology MIB)

- RFC 2737 (Entity MIB)
- RFC 2863 (Interfaces MIB)
- ANSI/TIA-1057/D6 (LLDP-MED; refer to “LLDP-MED (Media-Endpoint-Discovery)” on page 14-56.)

LLDP Operating Rules

(For additional information specific to LLDP-MED operation, refer to “LLDP-MED (Media-Endpoint-Discovery)” on page 14-56.)

Port Trunking. LLDP manages trunked ports individually. That is, trunked ports are configured individually for LLDP operation, in the same manner as non-trunked ports. Also, LLDP sends separate advertisements on each port in a trunk, and not on a per-trunk basis. Similarly, LLDP data received through trunked ports is stored individually, per-port.

IP Address Advertisements. In the default operation, if a port belongs to only one static VLAN, then the port advertises the lowest-order IP address configured on that VLAN. If a port belongs to multiple VLANs, then the port advertises the lowest-order IP address configured on the VLAN with the lowest VID. If the qualifying VLAN does not have an IP address, the port advertises 127.0.0.1 as its IP address. For example, if the port is a member of the default VLAN (VID = 1), and there is an IP address configured for the default VLAN, then the port advertises this IP address. In the default operation, the IP address that LLDP uses can be an address acquired by DHCP or Bootp.

You can override the default operation by configuring the port to advertise any IP address that is manually configured on the switch, even if the port does not belong to the VLAN configured with the selected IP address (page 14-53). (Note that LLDP cannot be configured through the CLI to advertise an addresses acquired through DHCP or Bootp. However, as mentioned above, in the default LLDP configuration, if the lowest-order IP address on the VLAN with the lowest VID for a given port is a DHCP or Bootp address, then the switch includes this address in its LLDP advertisements unless another address is configured for advertisements on that port.) Also, although LLDP allows configuring multiple remote management addresses on a port, only the lowest-order address configured on the port will be included in outbound advertisements. Attempting to use the CLI to configure LLDP with an IP address that is either not configured on a VLAN, or has been acquired by DHCP or Bootp results in the following error message.

```
xxx.xxx.xxx.xxx: This IP address is not configured or is  
a DHCP address.
```

Spanning-Tree Blocking. Spanning tree does not prevent LLDP packet transmission or receipt on STP-blocked links.

802.1X Blocking. Ports blocked by 802.1X operation do not allow transmission or receipt of LLDP packets.

Configuring LLDP Operation

In the default configuration, LLDP is enabled and in both transmit and receive mode on all active ports. The LLDP configuration includes global settings that apply to all active ports on the switch, and per-port settings that affect only the operation of the specified ports.

The commands in this section affect both LLDP and LLDP-MED operation. For information on operation and configuration unique to LLDP-MED, refer to “LLDP-MED (Media-Endpoint-Discovery)” on page 14-56.

Command	Page
show lldp config	14-47
[no] lldp run	14-47
lldp refresh-interval	14-48
lldp holdtime-multiplier	14-49
lldpTxDelay	14-49
lldpReinitDelay	14-50
lldp enable-notification	14-51
lldpnotificationinterval	14-52
lldp admin-status < txonly rxonly tx_rx disable >	14-52
lldp config < port-list > IpAddrEnable	14-53
lldp config < port-list > basicTlvEnable	14-54
lldp config < port-list > dot3TlvEnable < macphy_config >	14-56

Viewing the Current Configuration

Displaying the Global LLDP, Port Admin, and SNMP Notification

Status. This command displays the switch’s general LLDP configuration status, including some per-port information affecting advertisement traffic and trap notifications.

Syntax show lldp config

Displays the LLDP global configuration, LLDP port status, and SNMP notification status. For information on port admin status, refer to “Configuring Per-Port Transmit and Receive Modes” on page 14-52.

For example, **show lldp config** produces the following display when the switch is in the default LLDP configuration:

```
ProCurve(config)# show lldp config

LLDP Global Configuration

LLDP Enabled [Yes] : Yes
LLDP Transmit Interval [30] : 30
LLDP Hold time Multiplier [4] : 4
LLDP Delay Interval [2] : 2
LLDP Reinit Interval [2] : 2
LLDP Notification Interval [5] : 5

LLDP Port Configuration

Port | AdminStatus NotificationEnabled
-----+-----
1 | Tx_Rx False
2 | Tx_Rx False
3 | Tx_Rx False
4 | Tx_Rx False
5 | Tx_Rx False
6 | Tx_Rx False
7 | Tx_Rx False
8 | Tx_Rx False
. | .
. | .

Med Topology Trap Enabled
-----
False
True
False
False
True
False
False
```

Note: This value corresponds to the lldp refresh-interval command (page 14-48).

Figure 14-16. Example of Viewing the General LLDP Configuration

Displaying Port Configuration Details. This command displays the port-specific configuration, including.

Syntax show lldp config < port-list >

Displays the LLDP port-specific configuration for all ports in < port-list>, including which optional TLVs and any non-default IP address that are included in the port's outbound advertisements. For information on the notification setting, refer to "Configuring SNMP Notification Support" on page 14-51. For information on the other configurable settings displayed by this command, refer to "Configuring Per-Port Transmit and Receive Modes" on page 14-52.

```

ProCurve(config)# show lldp config a1

LLDP Port Configuration Detail

Port : a1
AdminStatus [Tx_Rx] : Tx_Rx
NotificationEnabled [False] : False
Med Topology Trap Enabled [False] : False

TLVS Advertised:
 * port_descr
 * system_name
 * system_descr
 * system_cap

[ * capabilities
 * network_policy |
 * location_id |
 * poe ]
[ * macphy_config ]

IpAddress Advertised:

```

These fields appear when medtlvenable is enabled on the switch, which is the default setting.

This field appears when dot3tlvenable is enabled on the switch, which is the default setting.

The blank IpAddress field indicates that the default IP address will be advertised from this port. (Refer to page 14-53: "Configuring a Remote Management Address for Outbound LLDP Advertisements")

Figure 14-17. Example of Per-Port Configuration Display

Configuring Global LLDP Packet Controls

The commands in this section configure the aspects of LLDP operation that apply the same to all ports in the switch.

Enabling or Disabling LLDP Operation on the Switch. Enabling LLDP operation (the default) causes the switch to:

- Use active, LLDP-enabled ports to transmit LLDP packets describing itself to neighbor devices.

- Add entries to its neighbors table based on data read from incoming LLDP advertisements.

Syntax [no] lldp run

Enables or disables LLDP operation on the switch. The **no** form of the command, regardless of individual LLDP port configurations, prevents the switch from transmitting outbound LLDP advertisements, and causes the switch to drop all LLDP advertisements received from other devices. The switch preserves the current LLDP configuration when LLDP is disabled. After LLDP is disabled, the information in the LLDP neighbors database remains until it times-out. (Default: Enabled)

For example, to disable LLDP on the switch:

```
ProCurve(config)# no lldp run
```

Changing the Packet Transmission Interval. This interval controls how often active ports retransmit advertisements to their neighbors.

Syntax lldp refresh-interval < 5 - 32768 >

Changes the interval between consecutive transmissions of LLDP advertisements on any given port. (Default: 30 seconds)

Note: The **refresh-interval** must be greater than or equal to (4 x **delay-interval**). (The default **delay-interval** is 2). For example, with the default **delay-interval**, the lowest **refresh-interval** you can use is 8 seconds (4 x 2 = 8). Thus, if you want a **refresh-interval** of 5 seconds, you must first change the delay interval to 1 (that is, 4 x 1 < 5). If you want to change the **delay-interval**, use the **setmib** command.

Changing the Time-to-Live for Transmitted Advertisements. The Time-to-Live value (in seconds) for all LLDP advertisements transmitted from a switch is controlled by the switch that generates the advertisement, and determines how long an LLDP neighbor retains the advertised data before discarding it. The Time-to-Live value is the result of multiplying the **refresh-interval** by the **holdtime-multiplier** described below.

Syntax `lldp holdtime-multiplier < 2 - 10 >`

Changes the multiplier an LLDP switch uses to calculate the Time-to-Live for the LLDP advertisements it generates and transmits to LLDP neighbors. When the Time-to-Live for a given advertisement expires the advertised data is deleted from the neighbor switch's MIB. (Default: 4; Range: 2 - 10)

For example, if the refresh-interval on the switch is 15 seconds and the **holdtime-multiplier** is at the default, the Time-to-Live for advertisements transmitted from the switch is 60 seconds (4 x 15). To reduce the Time-to-Live, you could lower the **holdtime-interval** to 2, which would result in a Time-to-Live of 30 seconds.

```
ProCurve(config)# lldp holdtime-multiplier 2
```

Changing the Delay Interval Between Advertisements Generated by Value or Status Changes to the LLDP MIB. The switch uses a *delay-interval* setting to delay transmitting successive advertisements resulting from these LLDP MIB changes. If a switch is subject to frequent changes to its LLDP MIB, lengthening this interval can reduce the frequency of successive advertisements. The delay-interval can be changed using either an SNMP network management application or the CLI **setmib** command.

Syntax `setmib lldpTxDelay.0 -i < 1 - 8192 >`

Uses **setmib** to change the minimum time (delay-interval) any LLDP port will delay advertising successive LLDP advertisements due to a change in LLDP MIB content. (Default: 2; Range: 1 - 8192)

Note: The LLDP refresh-interval (transmit interval) must be greater than or equal to (4 x delay-interval). The switch does not allow increasing the delay interval to a value that conflicts with this relationship. That is, the switch displays **Inconsistent value** if (4 x delay-interval) exceeds the current transmit interval, and the command fails. Depending on the current refresh-interval setting, it may be necessary to increase the refresh-interval before using this command to increase the delay-interval.

For example, to change the delay-interval from 2 seconds to 8 seconds when the refresh-interval is at the default 30 seconds, you must first set the refresh-interval to a minimum of 32 seconds ($32 = 4 \times 8$).

```
ProCurve(config)# setmib lldptxdelay.0 -i 8
lldptxdelay.0: Inconsistent value.
ProCurve(config)# lldp refresh-interval 32
ProCurve(config)# setmib lldptxdelay.0 -i 8
lldpTxDelay.0 = 8
```

Attempt to change the transmit-delay interval shows that the refresh-interval is less than (4 x delay-interval).

Successfully changes the transmit-delay interval to 8.

Changes the refresh-interval to 32; that is: $32 = 4 \times (\text{desired transmit-delay interval})$

Figure 14-18. Example of Changing the Transmit-Delay Interval

Changing the Reinitialization Delay Interval. In the default configuration, a port receiving a **disable** command followed immediately by a **txonly**, **rxonly**, or **tx_rx** command delays reinitializing for two seconds, during which time LLDP operation remains disabled. If an active port is subjected to frequent toggling between the LLDP disabled and enabled states, LLDP advertisements are more frequently transmitted to the neighbor device. Also, the neighbor table in the adjacent device will change more frequently, as it deletes, then replaces LLDP data for the affected port which, in turn, generates SNMP traps (if trap receivers and SNMP notification are configured). All of this can unnecessarily increase network traffic. Extending the reinitialization-

delay interval delays the port's ability to reinitialize and generate LLDP traffic following an LLDP disable/enable cycle.

Syntax `setmib lldpreinitdelay.0 -i < 1 - 10 >`

Uses **setmib** to change the minimum time (reinitialization delay interval) an LLDP port will wait before reinitializing after receiving an LLDP disable command followed closely by a `txonly` or `tx_rx` command. The delay interval commences with execution of the **lldp admin-status < port-list > disable** command. (Default: 2 seconds; Range: 1 - 10 seconds)

For example, the following command changes the reinitialization delay interval to five seconds:

```
ProCurve(config)# setmib lldpreinitdelay.0 -i 5
```

Configuring SNMP Notification Support

You can enable SNMP trap notification of LLDP data changes detected on advertisements received from neighbor devices, and control the interval between successive notifications of data changes on the same neighbor.

Enabling LLDP Data Change Notification for SNMP Trap Receivers.

Syntax `[no] lldp enable-notification < port-list >`

Enables or disables each port in `< port-list >` for sending notification to configured SNMP trap receiver(s) if an LLDP data change is detected in an advertisement received on the port from an LLDP neighbor. (Default: Disabled)

For information on configuring trap receivers in the switch, refer to “SNMP Notifications” on page 14-17.

For example, this command enables SNMP notification on ports 1 - 5:

```
ProCurve(config)# lldp enable-notification 1-5
```

Changing the Minimum Interval for Successive Data Change Notifications for the Same Neighbor.

If LLDP trap notification is enabled on a port, a rapid succession of changes in LLDP information received in advertisements from one or more neighbors can generate a high number of traps. To reduce this effect, you can globally change the interval between successive notifications of neighbor data change.

Syntax `setmib lldpnotificationinterval.0 -i < 1 - 3600 >`

Globally changes the interval between successive traps generated by the switch. If multiple traps are generated in the specified interval, only the first trap will be sent. The remaining traps will be suppressed. (A network management application can periodically check the switch MIB to detect any missed change notification traps. Refer to IEEE P802.1AB or later for more information.) (Default: 5 seconds)

For example, the following command limits change notification traps from a particular switch to one per minute.

```
ProCurve(config)# setmib lldpnotificationinterval.0 -i 60  
lldpNotificationInterval.0 = 60
```

Configuring Per-Port Transmit and Receive Modes

These commands control advertisement traffic inbound and outbound on active ports.

Syntax `lldp admin-status < port-list > < txonly | rxonly | tx_rx | disable >`

With LLDP enabled on the switch in the default configuration, each port is configured to transmit and receive LLDP packets. These options enable you to control which ports participate in LLDP traffic and whether the participating ports allow LLDP traffic in only one direction or in both directions.

txonly: *Configures the specified port(s) to transmit LLDP packets, but block inbound LLDP packets from neighbor devices.*

rxonly: *Configures the specified port(s) to receive LLDP packets from neighbors, but block outbound packets to neighbors.*

tx_rx: *Configures the specified port(s) to both transmit and receive LLDP packets. (This is the default setting.)*

disable: *Disables LLDP packet transmit and receive on the specified port(s).*

Configuring Basic LLDP Per-Port Advertisement Content

In the default LLDP configuration, outbound advertisements from each port on the switch include both mandatory and optional data.

Mandatory Data. An active LLDP port on the switch always includes the mandatory data in its outbound advertisements. LLDP collects the mandatory data, and, except for the Remote Management Address, you cannot use LLDP commands to configure the actual data.

- Chassis Type (TLV subelement)
- Chassis ID (TLV)
- Port Type (TLV subelement)
- Port ID (TLV)
- Remote Management Address (TLV; actual IP address is a subelement that can be a default address or a configured address)

Configuring a Remote Management Address for Outbound LLDP Advertisements. This is an optional command you can use to include a specific IP address in the outbound LLDP advertisements for specific ports.

Syntax [no] lldp config < port-list > ipAddrEnable < ip-address >

Replaces the default IP address for the port with an IP address you specify. This can be any IP address configured in a static VLAN on the switch, even if the port does not belong to the VLAN configured with the selected IP address. The **no** form of the command deletes the specified IP address. If there are no IP addresses configured as management addresses, then the IP address selection method returns to the default operation. (Default: The port advertises the IP address of the lowest-numbered VLAN (VID) to which it belongs. If there is no IP address configured on the VLAN(s) to which the port belongs, and the port is not configured to advertise an IP address from any other (static) VLAN on the switch, then the port advertises an address of 127.0.0.1.)

Note: This command does not accept either IP addresses acquired through DHCP or Bootp, or IP addresses that are not configured in a static VLAN on the switch

For example, if port 3 belongs to a subnetted VLAN that includes an IP address of 10.10.10.100 and you wanted port 3 to use this secondary address in LLDP advertisements, you would need to execute the following command:

```
ProCurve(config)# lldp config 3 ipAddrEnable 10.10.10.100
```

Optional Data. You can configure an individual port or group of ports to exclude one or more of these data types from outbound LLDP advertisements. Note that optional data types, when enabled, are populated with data internal to the switch; that is, you cannot use LLDP commands to configure their actual content.

- port description (TLV)
- system name (TLV)
- system description (TLV)
- system capabilities (TLV)
 - system capabilities Supported (TLV subelement)
 - system capabilities Enabled (TLV subelement)
- port speed and duplex (TLV subelement)

Syntax: [no] lldp config < port-list > basicTlvEnable < TLV-Type >

port_descr

For outbound LLDP advertisements, this TLV includes an alphanumeric string describing the port.
(Default: Enabled)

system_name

For outbound LLDP advertisements, this TLV includes an alphanumeric string showing the system's assigned name.
(Default: Enabled)

system_descr

For outbound LLDP advertisements, this TLV includes an alphanumeric string describing the full name and version identification for the system's hardware type, software version, and networking application.
(Default: Enabled)

system_cap

*For outbound advertisements, this TLV includes a bitmask of supported system capabilities (device functions). Also includes information on whether the capabilities are enabled.
(Default: Enabled)*

For example, if you wanted to exclude the system name TLV from the outbound LLDP advertisements for all ports on a switch, you would use this command:

```
ProCurve(config)# no lldp config 1-24 basicTlvEnable  
system_name
```

If you later decided to reinstate the system name TLV on ports 1-5, you would use this command:

```
ProCurve(config)# lldp config 1-5 basicTlvEnable  
system_name
```

Configuring Support for Port Speed and Duplex Advertisements

This feature is optional for LLDP operation, but is *required* for LLDP-MED operation.

Port speed and duplex advertisements are supported on the switches covered in this guide to inform an LLDP endpoint and the switch port of each other's port speed and duplex configuration and capabilities. Configuration mismatches between a switch port and an LLDP endpoint can result in excessive collisions and voice quality degradation. LLDP enables discovery of such mismatches by supporting SNMP access to the switch MIB for comparing the current switch port and endpoint settings. (Changing a current device configuration to eliminate a mismatch requires intervention by the system operator.)

Syntax: [no] lldp config < port-list > dot3TlvEnable macphy_config

For outbound advertisements, this TLV includes the (local) switch port's current speed and duplex settings, the range of speed and duplex settings the port supports, and the method required for reconfiguring the speed and duplex settings on the device (auto-negotiation during link initialization, or manual configuration).

*Using SNMP to compare local and remote information can help in locating configuration mismatches.
(Default: Enabled)*

Note: For LLDP operation, this TLV is optional. For LLDP-MED operation, this TLV is mandatory.

As mentioned above, an SNMP network management application can be used to compare the port speed and duplex data configured in the switch and advertised by the LLDP endpoint. You can also use the CLI to display this information. For more on using the CLI to display port speed and duplex information, refer to “Displaying the Current Port Speed and Duplex Configuration on a Switch Port” on page 14-72.

LLDP-MED (Media-Endpoint-Discovery)

LLDP-MED (ANSI/TIA-1057/D6) extends the LLDP (IEEE 802.1AB) industry standard to support advanced features on the network edge for Voice Over IP (VoIP) endpoint devices with specialized capabilities and LLDP-MED standards-based functionality. LLDP-MED in the switches uses the standard LLDP commands described earlier in this section, with some extensions, and also introduces new commands unique to LLDP-MED operation. The **show** commands described elsewhere in this section are applicable to both LLDP and LLDP-MED operation. LLDP-MED benefits include:

- plug-and-play provisioning for MED-capable, VoIP endpoint devices
- simplified, vendor-independent management enabling different IP telephony systems to interoperate on one network
- automatic deployment of convergence network policies (voice VLANs, Layer 2/CoS priority, and Layer 3/QoS priority)
- configurable endpoint location data to support the Emergency Call Service (ECS) (such as Enhanced 911 service, 999, 112)
- detailed VoIP endpoint data inventory readable via SNMP from the switch

- Power over Ethernet (PoE) status and troubleshooting support via SNMP
- support for IP telephony network troubleshooting of call quality issues via SNMP

This section describes how to configure and use LLDP-MED features in the switches to support VoIP network edge devices (Media Endpoint Devices) such as:

- IP phones
- voice/media gateways
- media servers
- IP communications controllers
- other VoIP devices or servers

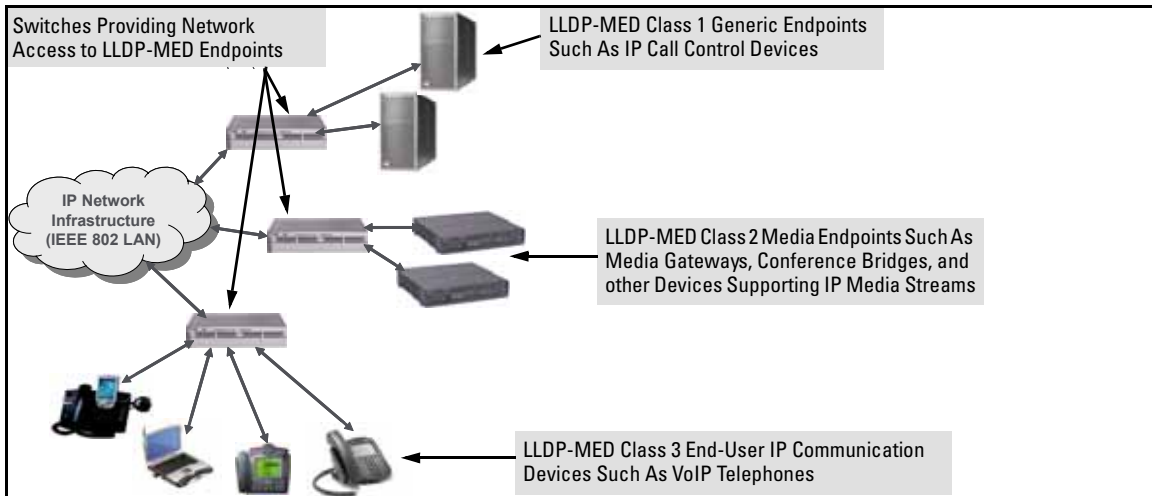


Figure 14-19. Example of LLDP-MED Network Elements

LLDP-MED Endpoint Support. LLDP-MED on the switches covered in this guide interoperates with directly connected IP telephony (endpoint) clients having these features and services:

- able to autonegotiate speed and duplex configuration with the switch

Configuring for Network Management Applications

LLDP (Link-Layer Discovery Protocol)

- able to use the following network policy elements configured on the client port
 - voice VLAN ID
 - 802.1p (Layer 2) QoS
 - Diffserv codepoint (DSCP) (Layer 3) QoS
- discover and advertise device location data learned from the switch
- support emergency call service (ECS—such as E911, 999, and 112)
- advertise device information for the device data inventory collected by the switch, including:
 - hardware revision
 - serial number
 - asset ID
 - firmware revision
 - manufacturer name
 - software revision
 - model name
- provide information on network connectivity capabilities (for example, a multi-port VoIP phone with Layer 2 switch capability)
- support the fast start capability

Note

LLDP-MED on the switches covered in this guide is intended for use with VoIP endpoints, and is not designed to support links between network infrastructure devices, such as switch-to-switch or switch-to-router links.

LLDP-MED Endpoint Device Classes. LLDP-MED endpoint devices are, by definition, located at the network edge and communicate using the LLDP-MED framework. Any LLDP-MED endpoint device belongs to one of the following three classes:

- Class 1 (Generic Endpoint Devices): These devices offer the basic LLDP discovery services, network policy advertisement (VLAN ID, Layer 2/802.1p priority, and Layer 3/DSCP priority), and PoE management. This class includes such devices as IP call controllers and communication-related servers.
- Class 2 (Media Endpoint Devices): These devices offer all Class 1 features plus media streaming capability, and include such devices as voice/media gateways, conference bridges, and media servers.

- Class 3 (Communication Devices): These devices are typically IP phones or end-user devices that otherwise support IP media and offer all Class 1 and Class 2 features, plus location identification and emergency 911 capability, Layer 2 switch support, and device information management.

LLDP-MED Operational Support. The switches covered in this guide offer two configurable TLVs supporting MED-specific capabilities:

- medTlvEnable (for per-port enabling or disabling of LLDP-MED operation)
- medPortLocation (for configuring per-port location or emergency call data)

Note

LLDP-MED operation also requires the port speed and duplex TLV (dot3TlvEnable; page 14-56), which is enabled in the default configuration.

LLDP-MED Topology Change Notification

This optional feature provides information an SNMP application can use to track LLDP-MED connects and disconnects.

Syntax: `lldp top-change-notify < port-list >`

Topology change notification, when enabled on an LLDP port, causes the switch to send an SNMP trap if it detects LLDP-MED endpoint connection or disconnection activity on the port, or an age-out of the LLDP-MED neighbor on the port. The trap includes the following information:

- *the port number (internal) on which the activity was detected (For more in internal port numbers, refer to “Determining the Switch Port Number Included in Topology Change Notification Traps” on page 14-78.)*
- *the LLDP-MED class of the device detected on the port (“LLDP-MED Endpoint Device Classes” on page 14-58.)*

The **show running** command shows whether the topology change notification feature is enabled or disabled. For example, if ports A1-A10 have topology change notification enabled, the following entry appears in the **show running** output:

```
lldp top-change-notify A1-A10
```

(Default: Disabled)

Note: To send traps, this feature requires access to at least one SNMP server. For information on configuring traps, refer to “SNMP Notifications” on page 14-17.

Also, if a detected LLDP-MED neighbor begins sending advertisements without LLDP-MED TLVs, the switch sends a top-change-notify trap.

Note

Topology change notifications provide one method for monitoring system activity. However, because SNMP normally employs UDP, which does not guarantee datagram delivery, topology change notification should not be relied upon as the sole method for monitoring critical endpoint device connectivity.

LLDP-MED Fast Start Control

Syntax: `lldp fast-start-count < 1 - 10 >`

*An LLDP-MED device connecting to a switch port may use the data contained in the MED TLVs from the switch to configure itself. However, the **lldp refresh-interval** setting (default: 30 seconds) for transmitting advertisements can cause an unacceptable delay in MED device configuration. To support rapid LLDP-MED device configuration, the **lldp fast-start-count** command temporarily overrides the **refresh-interval** setting for the **fast-start-count** advertisement interval. This results in the port initially advertising LLDP-MED at a faster rate for a limited time. Thus, when the switch detects a new LLDP-MED device on a port, it transmits one LLDP-MED advertisement per second out the port for the duration of the **fast-start-count** interval. In most cases, the default setting should provide an adequate **fast-start-count** interval.*

(Range: 1 - 10 seconds; Default: 5 seconds)

Note: This global command applies only to ports on which a new LLDP-MED device is detected. It does not override the refresh-interval setting on ports where non-MED devices are detected.

Advertising Device Capability, Network Policy, PoE Status and Location Data

The `medTlvEnable` option on the switch is enabled in the default configuration and supports the following LLDP-MED TLVs:

- LLDP-MED capabilities: This TLV enables the switch to determine:
 - whether a connected endpoint device supports LLDP-MED
 - which specific LLDP-MED TLVs the endpoint supports
 - the device class (1, 2, or 3) for the connected endpoint

This TLV also enables an LLDP-MED endpoint to discover what LLDP-MED TLVs the switch port currently supports.

- network policy operating on the port to which the endpoint is connected (VLAN, Layer 2 QoS, Layer 3 QoS)
- PoE (MED Power-over-Ethernet)
- physical location data — page 14-65

Note

LLDP-MED operation requires the `macphy_config` TLV subelement—enabled by default—that is optional for IEEE 802.1AB LLDP operation. Refer to the **`dot3TlvEnable macphy_config`** command on page 14-56.

Network Policy Advertisements. Network policy advertisements are intended for real-time voice and video applications, and include these TLV subelements:

- Layer 2 (802.1p) QoS
- Layer 3 DSCP (diffserv code point) QoS
- Voice VLAN ID (VID)

VLAN Operating Rules. These rules affect advertisements of VLANs in network policy TLVs:

- The VLAN ID TLV subelement applies only to a VLAN configured for voice operation (**`vlan < vid > voice`**).
- If there are multiple voice VLANs configured on a port, LLDP-MED advertises the voice VLAN having the lowest VID.
- The voice VLAN port membership configured on the switch can be tagged or untagged. However, if the LLDP-MED endpoint expects a tagged membership when the switch port is configured for untagged, or the reverse, then a configuration mismatch results. (Typically, the endpoint expects the switch port to have a tagged voice VLAN membership.)
- If a given port does not belong to a voice VLAN, then the switch does not advertise the VLAN ID TLV through this port.

Policy Elements. These policy elements may be statically configured on the switch or dynamically imposed during an authenticated session on the switch using a RADIUS server and 802.1X or MAC authentication. (Web authentication does not apply to VoIP telephones and other telecommunications devices that are not capable of accessing the switch through a Web browser.) The QoS and voice VLAN policy elements can be statically configured with the following CLI commands:

```
vlan < vid > voice
vlan < vid > < tagged | untagged > < port-list >
int < port-list > qos priority < 0 - 7 >
vlan < vid > qos dscp < codepoint >
```

Notes

A codepoint must have an 802.1p priority before you can configure it for use in prioritizing packets by VLAN-ID. If a codepoint you want to use shows **No Override** in the **Priority** column of the DSCP policy table (display with **show qos-dscp map**, then use **qos-dscp map < codepoint > priority < 0 - 7 >** to configure a priority before proceeding. For more on this topic, refer to the chapter titled “Quality of Service (QoS): Managing Bandwidth More Effectively” in the *Advanced Traffic Management Guide* for your switch.

Enabling or Disabling medTlvEnable. In the default LLDP-MED configuration, the TLVs controlled by medTlvEnable are enabled.

Syntax: [no] lldp config < port-list > medTlvEnable < medTlv >

- *Enables or disables advertisement of the following TLVs on the specified ports:*

- *device capability TLV*
- *configured network policy TLV*
- *configured location data TLV (Refer to “Configuring Location Data for LLDP-MED Devices” on page 14-65.)*
- *current PoE status TLV*

(Default: All of the above TLVs are enabled.)

- *Helps to locate configuration mismatches by allowing use of an SNMP application to compare the LLDP-MED configuration on a port with the LLDP-MED TLVs advertised by a neighbor connected to that port.*

capabilities

This TLV enables the switch to determine:

- *which LLDP-MED TLVs a connected endpoint can discover*
- *the device class (1, 2, or 3) for the connected endpoint*

This TLV also enables an LLDP-MED endpoint to discover what LLDP-MED TLVs the switch port currently supports.

(Default: enabled)

Note: This TLV cannot be disabled unless the network_policy, poe, and location_id TLVs are already disabled.

network-policy

This TLV enables the switch port to advertise its configured network policies (voice VLAN, Layer 2 QoS, Layer 3 QoS), and allows LLDP-MED endpoint devices to auto-configure the voice network policy advertised by the switch. This also enables the use of SNMP applications to troubleshoot statically configured endpoint network policy mismatches.

(Default: Enabled)

Notes: *Network policy is only advertised for ports that are configured as members of the voice VLAN. If the port belongs to more than one voice VLAN, then the voice VLAN with the lowest-numbered VID is selected as the VLAN for voice traffic. Also, this TLV cannot be enabled unless the capability TLV is already enabled.*

For more information, refer to “Network Policy Advertisements” on page 14-62

location_id

This TLV enables the switch port to advertise its configured location data (if any). For more on configuring location data, refer to “Configuring Location Data for LLDP-MED Devices”.

(Default: Enabled)

Note: *When disabled, this TLV cannot be enabled unless the capability TLV is already enabled.*

poe

This TLV enables the switch port to advertise its current PoE (Power over Ethernet) state and to read the PoE requirements advertised by the LLDP-MED endpoint device connected to the port.

(Default: Enabled)

Note: *When disabled, this TLV cannot be enabled unless the capability TLV is already enabled.*

For more on this topic, refer to “PoE Advertisements”, below.

PoE Advertisements. These advertisements inform an LLDP-MED endpoint of the power (PoE) configuration on switch ports. Similar advertisements from an LLDP-MED endpoint inform the switch of the endpoint's power needs and provide information that can be used to identify power priority mismatches.

Power-over-Ethernet TLVs include the following power data:

- **power type:** indicates whether the device is a power-sourcing entity (PSE) or a powered device (PD). Ports on the J8702A PoE zl module are PSE devices. A MED-capable VoIP telephone is a PD.
- **power source:** indicates the source of power in use by the device. Power sources for powered devices (PDs) include PSE, local (internal), and PSE/local. The switches covered in this guide advertise Unknown.
- **power priority:** indicates the power priority configured on the switch (PSE) port or the power priority configured on the MED-capable endpoint.
- **power value:** indicates the total power in watts that a switch port (PSE) can deliver at a particular time, or the total power in watts that the MED endpoint (PD) requires to operate.

To display the current power data for an LLDP-MED device connected to a port, use the following command:

```
show lldp info remote-device < port-list >
```

For more on this command, refer to page 14-73.

To display the current PoE configuration on the switch, use the following commands:

```
show power brief < port-list >
```

```
show power < port-list >
```

For more on PoE configuration and operation, refer to Chapter 11, “Power Over Ethernet (PoE) Operation”.

Configuring Location Data for LLDP-MED Devices

You can configure a switch port to advertise location data for the switch itself, the physical wall-jack location of the endpoint (recommended), or the location of a DHCP server supporting the switch and/or endpoint. You also have the option of configuring these different address types:

- **civic address:** physical address data such as city, street number, and building information

- **ELIN (Emergency Location Identification Number):** an emergency number typically assigned to MLTS (Multiline Telephone System Operators) in North America
- **coordinate-based location:** attitude, longitude, and altitude information (Requires configuration via an SNMP application.)

Syntax: [no] lldp config < port-list > medPortLocation < Address-Type >

*Configures location or emergency call data the switch advertises per port in the **location_id** TLV. This TLV is for use by LLDP-MED endpoints employing location-based applications.*

Note: *The switch allows one medPortLocation entry per port (without regard to type). Configuring a new medPortLocation entry of any type on a port replaces any previously configured entry on that port.*

civic-addr < COUNTRY-STR > < WHAT > < CA-TYPE > < CA-VALUE > ...
[< CA-TYPE > < CA-VALUE >] ... [< CA-TYPE > < CA-VALUE >]

This command enables configuration of a physical address on a switch port, and allows up to 75 characters of address information.

COUNTRY-STR: *A two-character country code, as defined by ISO 3166. Some examples include **FR** (France), **DE** (Germany), and **IN** (India). This field is required in a **civic-addr** command. (For a complete list of country codes, visit www.iso.org on the world wide web.)*

WHAT: *A single-digit number specifying the type of device to which the location data applies:*

0: *Location of DHCP server*

1: *Location of switch*

2: *Location of LLDP-MED endpoint (recommended application)*

*This field is required in a **civic-addr** command.*

—Continued—

— Continued—

Type/Value Pairs (CA-TYPE and CA-VALUE): This is a series of data pairs, each composed of a location data “type” specifier and the corresponding location data for that type. That is, the first value in a pair is expected to be the civic address “type” number (**CA-TYPE**), and the second value in a pair is expected to be the corresponding civic address data (**CA-VALUE**). For example, if the **CA-TYPE** for “city name” is “3”, then the type/value pair to define the city of Paris is “**3 Paris**”. Multiple type/value pairs can be entered in any order, although it is recommended that multiple pairs be entered in ascending order of the **CA-TYPE**. When an emergency call is placed from a properly configured class 3 endpoint device to an appropriate PSAP, the country code, device type, and type/value pairs configured on the switch port are included in the transmission. The “type” specifiers are used by the PSAP to identify and organize the location data components in an understandable format for response personnel to interpret. A **civic-addr** command requires a minimum of one type/value pair, but typically includes multiple type/value pairs as needed to configure a complete set of data describing a given location. **CA-TYPE:** This is the first entry in a type/value pair, and is a number defining the type of data contained in the second entry in the type/value pair (**CA-VALUE**). Some examples of **CA-TYPE** specifiers include:

- 3 = city
- 6 = street (name)
- 25 = building name

(Range: 0 - 255)

For a sample listing of **CA-TYPE** specifiers, refer to table 14-4 on page 14-69.

CA-VALUE: This is the second entry in a type/value pair, and is an alphanumeric string containing the location information corresponding to the immediately preceding **CA-TYPE** entry. Strings are delimited by either blank spaces, single quotes (‘...’), or double quotes (“...”). Each string should represent a specific data type in a set of unique type/value pairs comprising the description of a location, and each string must be preceded by a **CA-TYPE** number identifying the type of data in the string.

***Note:** A switch port allows one instance of any given **CA-TYPE**. For example, if a type/value pair of **6 Atlantic** (to specify “Atlantic” as a street name) is configured on port A5 and later another type/value pair of **6 Pacific** is configured on the same port, then **Pacific** replaces **Atlantic** in the civic address location configured for port A5.*

`elin-addr < emergency-number >`

This feature is intended for use in Emergency Call Service (ECS) applications to support class 3 LLDP-MED VoIP telephones connected to a switch covered in this guide in a multiline telephone system (MLTS) infrastructure. An ELIN (Emergency Location Identification Number) is a valid North American Numbering Plan (NANP) format telephone number assigned to MLTS operators in North America by the appropriate authority. The ELIN is used to route emergency (E911) calls to a Public Safety Answering Point (PSAP).

(Range: 1-15 numeric characters)

Configuring Coordinate-Based Locations. Latitude, longitude, and altitude data can be configured per switch port using an SNMP management application. For more information, refer to the documentation provided with the application. A further source of information on this topic is *RFC 3825-Dynamic Host Configuration Protocol Option for Coordinate-based Location Configuration Information*.

Note

Endpoint use of data from a medPortLocation TLV sent by the switch is device-dependent. Refer to the documentation provided with the endpoint device.

Table 14-4. Some Location Codes Used in CA-TYPE Fields*

Location Element	Code	Location Element	Code
national subdivision	1	street number	19
regional subdivision	2	additional location data	22
city or township	3	unit or apartment	26
city subdivision	4	floor	27
street	6	room number	28
street suffix	18		
<p>*The code assignments in this table are examples from a work-in-progress (the internet draft titled "Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information draft-ietf-geopriv-dhcp-civil-06" dated May 30, 2005.) For the actual codes to use, contact the PSAP or other authority responsible for specifying the civic addressing data standard for your network.</p>			

Example of a Location Configuration. Suppose a system operator wanted to configure the following information as the civic address for a telephone connected to her company's network through port A2 of a switch at the following location:

Description	CA-Type	CA-VALUE
national subdivision	1	CA
city	3	Widgitville
street	6	Main
street number	19	1433
unit	26	Suite 4-N
floor	27	4
room number	28	N4-3

Figure 14-20 shows the commands for configuring and displaying the above data.

```
ProCurve(config)# lldp config a2 medportlocation civic-addr US 2 1 CA
lle 6 Main 19 1433 26 Suite_4-N 27 4 28 N4-3
ProCurve(config)# show lldp config a2

LLDP Port Configuration Detail

Port : A2
AdminStatus [Tx_Rx] : Tx_Rx
NotificationEnabled [False] : False
Med Topology Trap Enabled [False] : False

Country Name      : US
What              : 2
Ca-Type           : 1
Ca-Length         : 2
Ca-Value          : CA
Ca-Type           : 3
Ca-Length         : 11
Ca-Value          : Widgitville
Ca-Type           : 6
Ca-Length         : 4
Ca-Value          : Main
Ca-Type           : 19
Ca-Length         : 4
Ca-Value          : 1433
Ca-Type           : 26
Ca-Length         : 9
Ca-Value          : Suite_4-N
Ca-Type           : 27
Ca-Length         : 1
Ca-Value          : 4
Ca-Type           : 28
```

Figure 14-20. Example of a Civic Address Configuration

Displaying Advertisement Data

Command	Page
show lldp info local-device	below
walkmib lldpXdot3LocPortOperMauType	
show lldp info remote-device	14-73
walkmib lldpXdot3RemPortAutoNegAdvertisedCap	
show lldp info stats	14-75

Displaying Switch Information Available for Outbound Advertisements

These commands display the current switch information that will be used to populate outbound LLDP advertisements.

Syntax `show lldp info local-device [port-list]`

Without the [port-list] option, this command displays the global switch information and the per-port information currently available for populating outbound LLDP advertisements.

With the [port-list] option, this command displays only the following port-specific information that is currently available for outbound LLDP advertisements on the specified ports:

- **PortType**
- **PortId**
- **PortDesc**

Note: This command displays the information available on the switch. Use the **lldp config < port-list >** command to change the selection of information that is included in actual outbound advertisements. In the default LLDP configuration, all information displayed by this command is transmitted in outbound advertisements.

For example, in the default configuration, the switch information currently available for outbound LLDP advertisements appears similar to the display in Figure 14-21 on page 14-72.

```

ProCurve(config)# show lldp info local-device

LLDP Local Device Information

Chassis Type : mac-address
Chassis Id   : 00 08 83 08 db 20
System Name  : ProCurve
System Description : HP J8697A ProCurve Switch 5406zl revision K.11.00 RO...
System Capabilities Supported : bridge, router
System Capabilities Enabled   : bridge
Management Address :
┌   Type:ipv4
└   Address: _ _ _ _ _

LLDP Port Information

Port      | PortType  PortId  PortDesc
-----+-----+-----+-----
1         | local     1       1
2         | local     2       2
3         | local     3       3
4         | local     4       4
5         | local     5       5
6         | local     6       6
.         | .         .       .
.         | .         .       .
.         | .         .       .

```

The Management Address field displays only the LLDP-configurable IP addresses on the switch. (Only manually-configured IP addresses are LLDP-configurable.) If the switch has only an IP address from a DHCP or Bootp server, then the Management Address field is empty (because there are no LLDP-configurable IP addresses available). For more on this topic, refer to "Remote Management Address" on page 14-43.

Figure 14-21. Example of Displaying the Global and Per-Port Information Available for Outbound Advertisements

```

ProCurve (config)# show lldp info local 1-2

LLDP Local Port Information Detail

Port      : 1
PortType  : local
PortId    : 1
PortDesc  : 1

-----

Port      : 2
PortType  : local
PortId    : 2
PortDesc  : 2

```

Figure 14-22. Example of the Default Per-Port Information Content for Ports 1 and 2

Displaying the Current Port Speed and Duplex Configuration on a Switch Port. Port speed and duplex information for a switch port and a connected LLDP-MED endpoint can be compared for configuration mismatches by using an SNMP application. You can also use the switch CLI to display this information, if necessary. The following two commands provide methods for displaying speed and duplex information for switch ports. For

information on displaying the currently configured port speed and duplex on an LLDP-MED endpoint, refer to “Displaying the Current Port Speed and Duplex Configuration on a Switch Port” on page 14-72.

Syntax: show interfaces brief < port-list >

*Includes port speed and duplex configuration in the **Mode** column of the resulting display.*

Displaying Advertisements Currently in the Neighbors MIB. These commands display the content of the inbound LLDP advertisements received from other LLDP devices.

Syntax show lldp info remote-device [port-list]

Without the [port-list] option, this command provides a global list of the individual devices it has detected by reading LLDP advertisements. Discovered devices are listed by the inbound port on which they were discovered. Multiple devices listed for a single port indicates that such devices are connected to the switch through a hub.

Discovering the same device on multiple ports indicates that the remote device may be connected to the switch in one of the following ways:

- Through different VLANs using separate links. (This applies to switches that use the same MAC address for all configured VLANs.)*
- Through different links in the same trunk.*
- Through different links using the same VLAN. (In this case, spanning-tree should be invoked to prevent a network topology loop. Note that LLDP packets travel on links that spanning-tree blocks for other traffic types.)*

With the [port-list] option, this command provides a listing of the LLDP data that the switch has detected in advertisements received on the specified ports.

For descriptions of the various types of information displayed by these commands, refer to Table 14-3 on page 14-42.

Configuring for Network Management Applications

LLDP (Link-Layer Discovery Protocol)

```
ProCurve# show lldp info remote

LLDP Remote Devices Information

LocalPort | ChassisId | PortId | PortName | SysName
-----+-----+-----+-----+-----
1 | 00 11 85 c6 54 60 | 17 | 17 | HP ProCurve Switch ...
2 | 00 11 85 cf 66 80 | 33 | 33 | HP ProCurve Switch ...
```

Figure 14-23. Example of a Global Listing of Discovered Devices

```
ProCurve(config)# show lldp info remote-device a2

LLDP Remote Device Information Detail

Local Port      : A2
ChassisType    : network-address
ChassisId      : 0f ff 7a 5c
PortType       : mac-address
PortId        : 08 00 0f 14 de f2
SysName        : regDN 3004.<IP-Phone-Data >
System Descr   : regDN 3004.<IP-Phone-Data >,h/w rev 0,ASIC rev 0,f/w Boot FW...
PortDescr     : LAN port

System Capabilities Supported : bridge, telephone
System Capabilities Enabled   : bridge, telephone

Remote Management Address

MED Information Detail
EndpointClass :Class3
Media Policy Vlan id :10
Media Policy Priority :7
Media Policy Dscp    :44
Media Policy Tagged  :False
Poe Device Type     :PD
Power Requested     :47
Power Source        :Unknown
Power Priority       :High
```

Indicates the policy configured on the telephone. A configuration mismatch occurs if the supporting port is configured differently.

Figure 14-24. Example of an LLLDP-MED Listing of an Advertisement Received From an LLDP-MED (VoIP Telephone) Source

Displaying LLDP Statistics

LLDP statistics are available on both a global and a per-port levels. Rebooting the switch resets the LLDP statistics counters to zero. Disabling the transmit and/or receive capability on a port “freezes” the related port counters at their current values.

Syntax `show lldp stats [port-list]`

The global LLDP statistics command displays an overview of neighbor detection activity on the switch, plus data on the number of frames sent, received, and discarded per-port. The per-port LLDP statistics command enhances the list of per-port statistics provided by the global statistics command with some additional per-port LLDP statistics.

Global LLDP Counters:

Neighbor Entries List Last Updated: *Shows the elapsed time since a neighbor was last added or deleted.*

New Neighbor Entries Count: *Shows the total of new LLDP neighbors detected since the last switch reboot. Disconnecting, then reconnecting a neighbor increments this counter.*

Neighbor Entries Deleted Count: *Shows the number of neighbor deletions from the MIB for AgeOut Count and forced drops for all ports. For example, if the admin status for port on a neighbor device changes from **tx_rx** or **txonly** to **disabled** or **rxonly**, then the neighbor device sends a “shutdown” packet out the port and ceases transmitting LLDP frames out that port. The device receiving the shutdown packet deletes all information about the neighbor received on the applicable inbound port and increments the counter.*

Neighbor Entries Dropped Count: *Shows the number of valid LLDP neighbors the switch detected, but could not add. This can occur, for example, when a new neighbor is detected when the switch is already supporting the maximum number of neighbors. Refer to “Neighbor Maximum” on page 14-77.*

Neighbor Entries AgeOut Count: *Shows the number of LLDP neighbors dropped on all ports due to Time-to-Live expiring.*

— Continued —

— Continued —

Per-Port LLDP Counters:

NumFramesRecvd: *Shows the total number of valid, inbound LLDP advertisements received from any neighbor(s) on < port-list >. Where multiple neighbors are connected to a port through a hub, this value is the total number of LLDP advertisements received from all sources.*

NumFramesSent: *Shows the total number of LLDP advertisements sent from < port-list >.*

NumFramesDiscarded: *Shows the total number of inbound LLDP advertisements discarded by < port-list >. This can occur, for example, when a new neighbor is detected on the port, but the switch is already supporting the maximum number of neighbors. Refer to “Neighbor Maximum” on page 14-77. This can also be an indication of advertisement formatting problems in the neighbor device.*

Frames Invalid: *Shows the total number of invalid LLDP advertisements received on the port. An invalid advertisement can be caused by header formatting problems in the neighbor device.*

TLVs Unrecognized: *Shows the total number of LLDP TLVs received on a port with a type value in the reserved range. This could be caused by a basic management TLV from a later LLDP version than the one currently running on the switch.*

TLVs Discarded: *Shows the total number of LLDP TLVs discarded for any reason. In this case, the advertisement carrying the TLV may be accepted, but the individual TLV was not usable.*

Neighbor Ageouts: *Shows the number of LLDP neighbors dropped on the port due to Time-to-Live expiring.*

```
ProCurve(config)# show lldp stats

LLDP Device Statistics

Neighbor Entries List Last Updated : 2 hours
New Neighbor Entries Count : 20
Neighbor Entries Deleted Count : 20
Neighbor Entries Dropped Count : 0
Neighbor Entries AgeOut Count : 20

LLDP Port Statistics
```

Port	NumFramesRecvd	NumFramesSent	NumFramesDiscarded
1	628	316	0
2	21	12	0
3	0	252	0
4	446	226	0
5	0	0	0
6	0	0	0
.	.	.	.
.	.	.	.
.	.	.	.

Counters showing frames sent on a port but no frames received on that port indicates an active link with a device that either has LLDP disabled on the link or is not LLDP-aware.

Figure 14-25. Example of a Global LLDP Statistics Display

```
ProCurve(config)# show lldp stats 1

LLDP Port Statistics Detail

PortName : 1
Frames Discarded : 0
Frames Invalid : 0
Frames Received : 658
Frames Sent : 331
TLVs Unrecognized : 0
TLVs Discarded : 0
Neighbor Ageouts : 0
```

Figure 14-26. Example of a Per-Port LLDP Statistics Display

LLDP Operating Notes

Neighbor Maximum. The neighbors table in the switch supports as many neighbors as there are ports on the switch. The switch can support multiple neighbors connected through a hub on a given port, but if the switch neighbor maximum is reached, advertisements from additional neighbors on the same or other ports will not be stored in the neighbors table unless some existing neighbors time-out or are removed.

LLDP Packet Forwarding: An 802.1D-compliant switch does not forward LLDP packets, regardless of whether LLDP is globally enabled or disabled on the switch.

One IP Address Advertisement Per-Port: LLDP advertises only one IP address per-port, even if multiple IP addresses are configured by **lldp config < port-list > ipAddrEnable** on a given port.

802.1Q VLAN Information. LLDP packets do not include 802.1Q header information, and are always handled as untagged packets.

Effect of 802.1X Operation. If 802.1X port security is enabled on a port and a connected device is not authorized, LLDP packets are not transmitted or received on that port. Any neighbor data stored in the neighbor MIB for that port prior to the unauthorized device connection remains in the MIB until it ages out. If an unauthorized device later becomes authorized, LLDP transmit and receive operation resumes.

Neighbor Data Can Remain in the Neighbor Database After the Neighbor Is Disconnected. After disconnecting a neighbor LLDP device from the switch, the neighbor can continue to appear in the switch's neighbor database for an extended period if the neighbor's **holdtime-multiplier** is high; especially if the **refresh-interval** is large. Refer to "Changing the Time-to-Live for Transmitted Advertisements" on page 14-49.

Mandatory TLVs. All mandatory TLVs required for LLDP operation are also mandatory for LLDP-MED operation.

Determining the Switch Port Number Included in Topology Change Notification Traps. Enabling topology change notification on a switch port and then connecting or disconnecting an LLDP-MED endpoint on that port causes the switch to send an SNMP trap to notify the designated management station(s). The port number included in the trap corresponds to the internal number the switch maintains for the designated port, and not the port's external (slot/number) identity. To match the port's external slot/number to the internal port number appearing in an SNMP trap, use the **walkmib ifDescr** command, as shown in the following figure:

```
ProCurve# walkmib ifDescr
┌ ifDescr.1 = A1 ───┐
│ ifDescr.2 = A2   │
│ ifDescr.3 = A3   │
│ .               │
│ .               │
│ ifDescr.23 = A23 │
│ ifDescr.24 = A24 │
│ ifDescr.27 = B1  │
│ ifDescr.28 = B2  │
│ ifDescr.29 = B3  │
│ .               │
│ .               │
│ ifDescr.48 = B22 │
│ ifDescr.49 = B23 │
│ ifDescr.50 = B24 │
│ .               │
│ .               │
└ ─── ─── ─── ───┘
```

Beginning and Ending of Port Number Listing for Slot A

Beginning and Ending of Port Number Listing for Slot B

Figure 14-27. Matching Internal Port Numbers to External Slot/Port Numbers

LLDP and CDP Data Management

This section describes points to note regarding LLDP (Link-Layer Discovery Protocol) and CDP (Cisco Discovery Protocol) data received by the switch from other devices. LLDP operation includes both transmitting LLDP packets to neighbor devices and reading LLDP packets received from neighbor devices. CDP operation is limited to reading incoming CDP packets from neighbor devices. (ProCurve switches do not generate CDP packets.)

LLDP and CDP Neighbor Data

With both LLDP and (read-only) CDP enabled on a switch port, the port can read both LLDP and CDP advertisements, and stores the data from both types of advertisements in its neighbor database. (The switch only *stores* CDP data that has a corresponding field in the LLDP neighbor database.) The neighbor database itself can be read by either LLDP or CDP methods or by using the **show lldp** commands. Take note of the following rules and conditions:

- If the switch receives both LLDP and CDP advertisements on the same port from the same neighbor the switch stores this information as two separate entries if the advertisements have differences chassis ID and port ID information.
- If the chassis and port ID information are the same, the switch stores this information as a single entry. That is, LLDP data overwrites the corresponding CDP data in the neighbor database if the chassis and port ID information in the LLDP and CDP advertisements received from the same device is the same.
- Data read from a CDP packet does not support some LLDP fields, such as “System Descr”, “SystemCapSupported”, and “ChassisType”. For such fields, LLDP assigns relevant default values. Also:
 - The LLDP “System Descr” field maps to CDP’s “Version” and “Platform” fields.
 - The switch assigns “ChassisType” and “PortType” fields as “local” for both the LLDP and the CDP advertisements it receives.
 - Both LLDP and CDP support the “System Capability” TLV. However, LLDP differentiates between what a device is capable of supporting and what it is actually supporting, and separates the two types of information into subelements of the System Capability TLV. CDP has only a single field for this data. Thus, when CDP System Capability data is mapped to LLDP, the same value appears in both LLDP System Capability fields.
 - System Name and Port Descr are not communicated by CDP, and thus are not included in the switch’s Neighbors database.

Note

Because ProCurve switches do not generate CDP packets, they are not represented in the CDP data collected by any neighbor devices running CDP.

A switch with CDP disabled forwards the CDP packets it receives from other devices, but does not store the CDP information from these packets in its own MIB.

LLDP data transmission/collection and CDP data collection are both enabled in the switch’s default configuration. In this state, an SNMP network management application designed to discover devices running either CDP or LLDP can retrieve neighbor information from the switch regardless of whether LLDP or CDP is used to collect the device-specific information.

Protocol State	Packet Generation	Inbound Data Management	Inbound Packet Forwarding
CDP Enabled ¹	n/a	Store inbound CDP data.	No forwarding of inbound CDP packets.
CDP Disabled	n/a	No storage of CDP data from neighbor devices.	Floods inbound CDP packets from connected devices to outbound ports.
LLDP Enabled ¹	Generates and transmits LLDP packets out all ports on the switch.	Store inbound LLDP data.	No forwarding of inbound LLDP packets.
LLDP Disabled	No packet generation.	No storage of LLDP data from neighbor devices.	No forwarding of inbound LLDP packets.

¹Both CDP data collection and LLDP transmit/receive are enabled in the default configuration. If a switch receives CDP packets and LLDP packets from the same neighbor device on the same port, it stores and displays the two types of information separately if the chassis and port ID information in the two types of advertisements is different. In this case, if you want to use only one type of data from a neighbor sending both types, disable the unwanted protocol on either the neighbor device or on the switch. However, if the chassis and port ID information in the two types of advertisements is the same, the LLDP information overwrites the CDP data for the same neighbor device on the same port.

CDP Operation and Commands

By default the switches covered in this guide have CDP enabled on each port. This is a read-only capability, meaning that the switch can receive and store information about adjacent CDP devices but does not generate CDP packets.

When a CDP-enabled switch receives a CDP packet from another CDP device, it enters that device's data in the CDP Neighbors table, along with the port number where the data was received (and does not forward the packet). The switch also periodically purges the table of any entries that have expired. (The hold time for any data entry in the switch's CDP Neighbors table is configured in the device transmitting the CDP packet, and cannot be controlled in the switch receiving the packet.) A switch reviews the list of CDP neighbor entries every three seconds, and purges any expired entries.

Command	Page
show cdp	14-82
show cdp neighbors [<i>< port-list > detail</i>] [detail <i>< port-list ></i>]	14-83
[no] cdp run	14-84
[no] cdp enable <i>< port-list ></i>	14-84

Note

For details on how to use an SNMP utility to retrieve information from the switch's CDP Neighbors table maintained in the switch's MIB (Management Information Base), refer to the documentation provided with the particular SNMP utility.

Viewing the Switch's Current CDP Configuration. CDP is shown as enabled/disabled both globally on the switch and on a per-port basis.

Syntax: show cdp

Lists the switch's global and per-port CDP configuration.

The following example shows the default CDP configuration.

```
ProCurve(config)# show cdp
Global CDP information
  Enable CDP [Yes] : Yes

Port CDP
-----
A1  enabled
A2  enabled
A3  enabled
.   .
.   .
.   .
```

Figure 14-28. Example of Show CDP with the Default CDP Configuration

Viewing the Switch's Current CDP Neighbors Table. Devices are listed by the port on which they were detected.

Syntax: show cdp neighbors

Lists the neighboring CDP devices the switch detects, with a subset of the information collected from the device's CDP packet.

[[e] port-numb [detail]]

*Lists the CDP device connected to the specified port. (Allows only one port at a time.) Using **detail** provides a longer list of details on the CDP device the switch detects on the specified port.*

[detail [[e] port-num]]

Provides a list of the details for all of the CDP devices the switch detects. Using port-num produces a list of details for the selected port.

Figure 14-29 lists CDP devices that the switch has detected by receiving their CDP packets.

```
ProCurve> show cdp neighbors
CDP neighbors information
```

Port	Device ID	Platform	Capability
A1	Accounting(0030c1-7fcc40)	J4812A ProCurve Switch...	S
A2	Research(0060b0-889e43)	J4121A ProCurve Switch...	S
A4	Support(0060b0-761a45)	J4121A ProCurve Switch...	S
A7	Marketing(0030c5-38dc59)	J4813A ProCurve Switch...	S
A12	Mgmt NIC(099a05-09df9b)	NIC Model X666	H
A12	Mgmt NIC(099a05-09df11)	NIC Model X666	H

Figure 14-29. Example of CDP Neighbors Table Listing

Enabling CDP Operation. Enabling CDP operation (the default) on the switch causes the switch to add entries to its CDP Neighbors table for any CDP packets it receives from other neighboring CDP devices.

Disabling CDP Operation. Disabling CDP operation clears the switch's CDP Neighbors table and causes the switch to drop inbound CDP packets from other devices without entering the data in the CDP Neighbors table.

Syntax: [no] cdp run

*Enables or disables CDP read-only operation on the switch.
(Default: Enabled)*

For example, to disable CDP read-only on the switch:

```
ProCurve(config)# no cdp run
```

When CDP is disabled:

- **show cdp neighbors** displays an empty CDP Neighbors table
- **show cdp** displays

```
Global CDP information
Enable CDP [Yes]: No
```

Enabling or Disabling CDP Operation on Individual Ports. In the factory-default configuration, the switch has all ports enabled to receive CDP packets. Disabling CDP on a port causes it to drop inbound CDP packets without recording their data in the CDP Neighbors table.

Syntax: [no] cdp enable < [e] port-list >

For example, to disable CDP on port A1:

```
ProCurve(config)# no cdp enable a1
```