

Port Status and Configuration

Contents

Overview	10-2
Viewing Port Status and Configuring Port Parameters	10-2
Menu: Port Configuration	10-5
CLI: Viewing Port Status and Configuring Port Parameters	10-7
Viewing Port Status and Configuration	10-7
Viewing Port Utilization Statistics	10-9
Viewing Transceiver Status	10-9
Enabling or Disabling Ports and Configuring Port Mode	10-11
Enabling or Disabling Flow Control	10-12
Configuring a Broadcast Limit on the Switch	10-14
Configuring ProCurve Auto-MDIX	10-15
Web: Viewing Port Status and Configuring Port Parameters	10-18
Using Friendly (Optional) Port Names	10-18
Configuring and Operating Rules for Friendly Port Names	10-18
Configuring Friendly Port Names	10-19
Displaying Friendly Port Names with Other Port Data	10-20
Configuring Transceivers and Modules That Haven't Been Inserted	10-23
Transceivers	10-23
Modules	10-23
Uni-Directional Link Detection (UDLD)	10-25
Configuring UDLD	10-26
Enabling UDLD	10-27
Changing the Keepalive Interval	10-28
Changing the Keepalive Retries	10-28
Configuring UDLD for Tagged Ports	10-28
Viewing UDLD Information	10-29

Configuration Warnings and Event Log Messages 10-31

Overview

This chapter describes how to view the current port configuration and how to configure ports to non-default settings, including

- Enable/Disable
- Mode (speed and duplex)
- Flow Control
- Broadcast Limit
- Friendly Port Names
- Uni-directional Link Detection (UDLD)

Viewing Port Status and Configuring Port Parameters

Port Status and Configuration Features

Feature	Default	Menu	CLI	Web
viewing port status	n/a	page 10-6	page 10-8	page 10-19
viewing transceiver status	n/a	n/a	page 10-10	page 10-19
configuring ports	Refer to Table 10-1 on pages 10-4 thru 10-6	page 10-7	page 10-12	page 10-19
configuring ProCurve auto-mdix			page 9-11	

Note On Connecting Transceivers to Fixed-Configuration Devices

If the switch either fails to show a link between an installed transceiver and another device, or demonstrates errors or other unexpected behavior on the link, check the port configuration on both devices for a speed and/or duplex (mode) mismatch.

- To check the mode setting for a port on the switch, use either the Port Status screen in the menu interface (page 10-6) or **show interfaces brief** in the CLI (page 10-8).

To display information about the transceivers installed on a switch, enter the **show tech receivers** command in the CLI (page 10-11).

Table 10-1. Status and Parameters for Each Port Type

Status or Parameter	Description
Enabled	<p>Yes (default): The port is ready for a network connection.</p> <p>No: The port will not operate, even if properly connected in a network. Use this setting, for example, if the port needs to be shut down for diagnostic purposes or while you are making topology changes.</p>
Status (read-only)	<p>Up: The port senses a link beat.</p> <p>Down: The port is not enabled, has no cables connected, or is experiencing a network error. For troubleshooting information, refer to the <i>Installation and Getting Started Guide</i> you received with the switch. Refer also to Appendix C, "Troubleshooting" (in this manual).</p>
Mode	The port's speed and duplex (data transfer operation) setting.

10/100/1000Base-T Ports:

- **Auto-MDIX** (default): Senses speed and negotiates with the port at the other end of the link for port operation (MDI-X or MDI).
To see what the switch negotiates for the Auto setting, use the CLI **show interfaces brief** command or the "3. Port Status" option under "1. Status and Counters" in the menu interface.
- **MDI**: Sets the port to connect with a PC using a crossover cable (Manual mode—applies only to copper port switches using twisted-pair copper Ethernet cables)
- **MDIX**: Sets the port to connect with a PC using a straight-through cable (Manual mode—applies only to copper port switches using twisted-pair copper Ethernet cables)
- **Auto-10**: Allows the port to negotiate between half-duplex (HDx) and full-duplex (FDx) while keeping speed at 10 Mbps. Also negotiates flow control (enabled or disabled). ProCurve recommends Auto-10 for links between 10/100 auto-sensing ports connected with Cat 3 cabling. (Cat 5 cabling is required for 100 Mbps links.)
- **10HDx**: 10 Mbps, Half-Duplex
- **10FDx**: 10 Mbps, Full-Duplex
- **Auto-100**: Uses 100 Mbps and negotiates with the port at the other end of the link for other port operation features.
- **Auto-10-100**: Allows the port to establish a link with the port at the other end at either 10 Mbps or 100 Mbps, using the highest mutual speed and duplex mode available. Only these speeds are allowed with this setting.
- **Auto-1000**: Uses 1000 Mbps and negotiates with the port at the other end of the link for other port operation features.
- **100Hdx**: Uses 100 Mbps, half-duplex.
- **100Fdx**: Uses 100 Mbps, Full-Duplex

— Continued on Next Page —

Status or Parameter	Description
---------------------	-------------

— Continued From Previous Page —

Gigabit Fiber-Optic Ports (Gigabit-SX, Gigabit-LX, and Gigabit-LH):

- **1000FDx:** 1000 Mbps (1 Gbps), Full Duplex only
- **Auto** (default): The port operates at 1000FDx and auto-negotiates flow control with the device connected to the port.

Gigabit Copper Ports:

- **1000FDx:** 1000 Mbps (1 Gbps), Full Duplex only
- **Auto** (default): The port operates at 1000FDx and auto-negotiates flow control with the device connected to the port.

10-Gigabit CX4 Copper Ports:

- **Auto:** The port operates at 10 gigabits FDx and negotiates flow control. Lower speed settings or half-duplex are not allowed.

10-Gigabit flexible media slots that support these X2 transceivers:

- ProCurve 10 GbE X2 SR-SC Xcvr
- ProCurve 10 GbE X2 LR-SC Xcvr
- ProCurve 10 GbE X2 ER-SC Xcvr
- ProCurve 10 GbE X2 CX4 media converter
- ProCurve 10 GbE X2 CS4 Xcvr.

10-Gigabit SC Fiber-Optic Ports (10-GbE SR, 10-GbE LR, 10-GbE ER):

- **Auto:** The port operates at 10 gigabits FDx and negotiates flow control. Lower speed settings or half-duplex are not allowed.

Note: Conditioning patch cord cables are not supported on 10-GbE.

Auto-MDIX	<p>The switch supports Auto-MDIX on 10Mb, 100Mb, and 1 Gb T/TX (copper) ports. (Fiber ports and 10-gigabit ports do not use this feature.)</p> <ul style="list-style-type: none"> • Automdix: Configures the port for automatic detection of the cable type (straight-through or crossover). • MDI: Configures the port to connect to a switch, hub, or other MDI-X device with a straight-through cable. • MDIX: Configures the port to connect to a PC or other MDI device with a straight-through cable.
-----------	---

Flow Control	<ul style="list-style-type: none"> • Disabled (default): The port does not generate flow control packets, and drops any flow control packets it receives. • Enabled: The port uses 802.3x Link Layer Flow Control, generates flow control packets, and processes received flow control packets.
--------------	---

With the port mode set to **Auto** (the default) and Flow Control enabled, the switch negotiates Flow Control on the indicated port. If the port mode is not set to Auto, or if Flow Control is disabled on the port, then Flow Control is not used. Note that flow control must be enabled on both ends of a link.

Status or Parameter	Description
Broadcast Limit	<p>Specifies the percentage of the theoretical maximum network bandwidth that can be used for broadcast and multicast traffic. Any broadcast or multicast traffic exceeding that limit will be dropped. Zero (0) means the feature is disabled.</p> <p>The broadcast-limit command operates at the port context level to set the broadcast limit for a port on the switch.</p> <p>Note: This feature is not appropriate for networks that require high levels of IPX or RIP broadcast traffic.</p>

Menu: Port Configuration

From the menu interface, you can view and change the port configuration.

Using the Menu To View Port Configuration. The menu interface displays the configuration for ports and (if configured) any trunk groups.

From the Main Menu, select:

1. Status and Counters
4. Port Status

```

----- CONSOLE - MANAGER MODE -----
                        Status and Counters - Port Status
-----
Port      Type      Intrusion  Enabled  Status  Mode  MDI  Flow
          Type      Alert      Status  Mode    Mode Ctrl
-----
B1        10/100TX  No         Yes     Down   10FDx Auto off
B2        10/100TX  No         Yes     Down   10FDx Auto off
B3        10/100TX  No         Yes     Down   10FDx Auto off
B4        10/100TX  No         Yes     Down   10FDx Auto off
B5        10/100TX  No         Yes     Down   10FDx Auto off
B6        10/100TX  No         Yes     Down   10FDx Auto off
B7-Trk2   10/100TX  No         Yes     Down   10FDx Auto off
B8-Trk2   10/100TX  No         Yes     Down   10FDx Auto off
B9        10/100TX  No         Yes     Down   10FDx Auto off
B10       10/100TX  No         Yes     Down   10FDx Auto off
B11       10/100TX  No         Yes     Down   10FDx Auto off

Actions->  Back  Intrusion log  Help

Return to previous screen.
Use up/down arrow keys to scroll to other entries, left/right arrow keys to
change action selection, and <Enter> to execute action.
    
```

In this example, ports A7 and A8 have previously been configured as a trunk group.

Figure 10-1. Example of a Switch Port Status Screen

Using the Menu To Configure Ports.

You can configure and view the port settings by using the menu.

Note

The menu interface uses the same screen for configuring both individual ports and port trunk groups. For information on port trunk groups, refer to Chapter 11, “Port Trunking” .

1. From the Main Menu, Select:

2. Switch Configuration...

2. Port/Trunk Settings

An example of the Menu display is shown below.

```
===== TELNET - MANAGER MODE =====
                Switch Configuration - Port/Trunk Settings

Port      Type      Enabled      Mode      Flow Ctrl  Group  Type
----      -+-----  -+-----  -+-----  -+-----  -+-----  -+-----
A1      1000T      | Yes      Auto-10-100  Disable
A2      1000T      | Yes      Auto-10-100  Disable
A3      1000T      | Yes      Auto          Disable
A4      1000T      | Yes      Auto          Disable
A5      1000T      | Yes      Auto          Disable
A6      1000T      | Yes      Auto          Disable
A7      1000T      | Yes      Auto          Disable      Trk1  Trunk
A8      1000T      | Yes      Auto          Disable      Trk2  Trunk

Actions->  Cancel      Edit      Save      Help

Cancel changes and return to previous screen.
Use arrow keys to change action selection and <Enter> to execute ac-
tion.
```

Figure 10-2. Example of Port/Trunk Settings with a Trunk Group Configured

2. Press **[E]** (for **E**dit). The cursor moves to the **Enabled** field for the first port.
3. Refer to the online help provided with this screen for further information on configuration options for these features.
4. When you have finished making changes to the above parameters, press **[Enter]**, then press **[S]** (for **S**ave).

CLI: Viewing Port Status and Configuring Port Parameters

From the CLI, you can configure and view all port parameter settings and view all port status indicators.

Port Status and Configuration Commands

show interfaces brief	page 10-9
show interfaces config	page 10-9
show interfaces port-utilization	page 10-10
show tech transceivers	page 10-10
interface	page 10-12
disable/enable	page 10-12
speed-duplex	page 10-12
flow-control	page 10-13
broadcast-limit	page 10-15
auto-mdix	page 10-16

Viewing Port Status and Configuration

Use the following commands to display port status and configuration data.

Syntax: show interfaces [brief | config | < port-list >]

brief: Lists the current operating status for all ports on the switch.

config: Lists a subset of configuration data for all ports on the switch; that is, for each port, the display shows whether the port is enabled, the operating mode, and whether it is configured for flow control.

< port-list >: Shows a summary of network traffic handled by the specified ports.

An example of the **show interfaces brief** command is shown below.

```
ProCurve(config)# show interfaces brief
Status and Counters - Port Status
```

Port	Type	Intrusion		Status	Mode	MDI Mode	Flow Ctrl	Bcast Limit
		Alert	Enabled					
B1	100/1000T	No	Yes	Down	Auto-10-100	Auto	off	0
B2	100/1000T	No	Yes	Down	1000FDx	Auto	off	0
B3	100/1000T	No	Yes	Down	1000FDx	Auto	off	0
B4	100/1000T	No	Yes	Down	1000FDx	Auto	off	0
B5	100/1000T	No	Yes	Down	1000FDx	Auto	off	0
B6	100/1000T	No	Yes	Down	1000FDx	Auto	off	0

Figure 10-3. Example of Show Interfaces Brief Command Listing

Use the **show interfaces config** command to view the port settings, as shown below.

```
ProCurve(config)# show interfaces config

Port Settings
```

Port	Type	Enabled	Mode	Flow Ctrl	MDI
B1	100/1000T	Yes	Auto-10-100	Disable	Auto
B2	100/1000T	Yes	Auto	Disable	Auto
B3	100/1000T	Yes	Auto	Disable	Auto
B4	100/1000T	Yes	Auto	Disable	Auto
B5	100/1000T	Yes	Auto	Disable	Auto
B6	100/1000T	Yes	Auto	Disable	Auto

Figure 10-4. Example of a Show Interfaces Config Command Listing

Viewing Port Utilization Statistics

Use the **show interface port-utilization** command to view a real-time rate display for all ports on the switch. The following shows a sample output from this command.

```
ProCurve(config)# show interfaces port-utilization
Status and Counters - Port Utilization
```

Port	Mode	Rx			Tx		
		Kbits/sec	Pkts/sec	Util	Kbits/sec	Pkts/sec	Util
B1	1000FDx	0	0	0	0	0	0
B2	1000FDx	0	0	0	0	0	0
B3	1000FDx	0	0	0	0	0	0
B4	1000FDx	0	0	0	0	0	0
B5	1000FDx	0	0	0	0	0	0
B6	1000FDx	0	0	0	0	0	0
B7	100FDx	624	86	00.62	496	0	00.49

Figure 10-5. Example of a Show Interface Port-Utilization Command Listing

Operating Notes:

- For each port on the switch, the command provides a real-time display of the rate at which data is received (Rx) and transmitted (Tx) in terms of kilobits per second (KBits/s), number of packets per second (Pkts/s), and utilization (Util) expressed as a percentage of the total bandwidth available.
- The **show interfaces <port-list>** command can be used to display the current link status and the port rate average over a 5 minute period. Port rates are shown in bits per second (bps) for ports up to 1 Gigabit; for 10 Gigabit ports, port rates are shown in kilobits per second (Kbps).

Viewing Transceiver Status

The **show tech transceivers** command allows you to:

- Remotely identify transceiver type and revision number without having to physically remove an installed transceiver from its slot.
- Display real-time status information about all installed transceivers, including non-operational transceivers.

Figure 10-6 shows sample output from the **show tech transceivers** command.

```
ProCurve# show tech transceivers

Transceiver Technical Information:
Port # | Type      | Prod # | Serial #      | Part #
-----+-----+-----+-----+-----
21     | 1000SX   | J4858B | CN605MP23K   |
22     | 1000LX   | J4859C | H117E7X      | 2157-2345
23     | ??       | ??     | non operational |
25     | 10GbE-CX4 | J8440A | US509RU079   |
26     | 10GbE-CX4 | J8440A | US540RU002   |
27     | 10GbE-LR | J8437B | PPA02-2904:0017 | 2157-2345
28     | 10GbE-SR | J8436B | 01591602     | 2158-1000
29     | 10GbE-ER | J8438A | PPA03-2905:0001 |

The following transceivers may not function correctly:
Port #      Message
-----+-----
Port 23     Self test failure.
```

Figure 10-6. Example of Show Tech Transceivers Command

Operating Notes:

- The following information is displayed for each installed transceiver:
 - Port number on which transceiver is installed.
 - Type of transceiver.
 - Product number—Includes revision letter, such as A, B, or C. If no revision letter follows a product number, this means that no revision is available for the transceiver.
 - Part number—Allows you to determine the manufacturer for a specified transceiver and revision number.
- For a non-ProCurve installed transceiver (see line 23 Figure 10-6), no transceiver type, product number, or part information is displayed. In the Serial Number field, **non-operational** is displayed instead of a serial number.
- The following error messages may be displayed for a non-operational transceiver:
 - Unsupported Transceiver. (SelfTest Err#060)
Check: www.hp.com/rnd/device_help/2_inform for more info.

Port Status and Configuration

Viewing Port Status and Configuring Port Parameters

- This switch only supports revision B and above transceivers. Check: www.hp.com/rnd/device_help/2_inform for more info.
- Self test failure.
- Transceiver type not supported in this port.
- Transceiver type not supported in this software version.
- Not a ProCurve Transceiver. Please go to: www.hp.com/rnd/device_help/2_inform for more info.

Enabling or Disabling Ports and Configuring Port Mode

You can configure one or more of the following port parameters. Refer to table 10-1 on pages 10-4 through 10-6.

Syntax: [no] interface <port-list>

[<disable | enable>]

*Disables or enables the port for network traffic. Does not use the **no** form of the command. (Default: **enable**.)*

[speed-duplex <auto-10 | 10-full | 10-half | 100-full | 100-half | auto | auto-100 | 1000-full >]

*Specifies the port's data transfer speed and mode. Does not use the **no** form of the command. (Default: **auto**.)*

Note that in the above syntax you can substitute an “**int**” for “**interface**”; that is: **int <port-list>**.

The 10/100 auto-negotiation feature allows a port to establish a link with a port at the other end at either 10 Mbps or 100 Mbps, using the highest mutual speed and duplex mode available. Only these speeds are allowed with this setting.

For example, to configure port C5 for auto-10-100, enter this command:

```
ProCurve(config)# int c5 speed-duplex auto-10-100
```

To configure ports C1 through C3 and port C6 for 100Mbps full-duplex, you would enter these commands:

```
ProCurve(config)# int c1-c3,c6 speed-duplex 100-full
```

Similarly, to configure a single port with the above command settings, you could either enter the same command with only the one port identified, or go to the *context level* for that port and then enter the command. For example, to enter the context level for port C6 and then configure that port for 100FDx:

```
ProCurve(config)# int e c6  
ProCurve(eth-C6)# speed-duplex 100-full
```

If port C8 was disabled, and you wanted to enable it and configure it for 100FDx with flow-control active, you could do so with either of the following command sets.

```
ProCurve(config)# int c8 enable  
ProCurve(config)# int c8 speed-duplex 100-full  
ProCurve(config)# int c8 flow-control  
  
ProCurve(eth-C8)# enable  
ProCurve(eth-C8)# speed-duplex 100-full
```

These commands enable and configure port C8 from the config level:

These commands select the port C8 context level and then apply the subsequent configuration commands to port C8:

Figure 10-7. Examples of Two Methods for Changing a Port Configuration

Refer to “Enabling or Disabling Flow Control” on page 10-13 for more on flow control.

Enabling or Disabling Flow Control

Note

You must enable flow control on both ports in a given link. Otherwise, flow control does not operate on the link, and appears as **Off** in the **show interfaces brief** port listing, even if flow control is configured as enabled on the port in the switch. (Refer to Figure 10-3 on page 10-9.) Also, the port (speed-duplex) mode must be set to **Auto** (the default).

To disable flow control on some ports, while leaving it enabled on other ports, just disable it on the individual ports you want to exclude.

Syntax: [no]interface < port-list > flow-control

Enables or disables flow control packets on the port. The “no” form of the command disables flow control on the individual ports. (Default: Disabled.)

For example, suppose that:

1. You want to enable flow control on ports A1-A6.
2. Later, you decide to disable flow control on ports A5 and A6.
3. As a final step, you want to disable flow control on all ports.

Assuming that flow control is currently disabled on the switch, you would use these commands:

```
ProCurve(config)# int a1-a6 flow-control
ProCurve(config)# show interfaces brief
Status and Counters - Port Status
```

Port	Type	Intrusion Alert	Enabled	Status	Mode	Flow Ctrl
A1	10/100TX	No	Yes	Up	10FDx	on
A2	10/100TX	No	Yes	Up	10FDx	on
A3	10/100TX	No	Yes	Up	10FDx	on
A4	10/100TX	No	Yes	Up	10FDx	on
A5	10/100TX	No	Yes	Up	10FDx	on
A6	10/100TX	No	Yes	Up	10FDx	on
A7	10/100TX	No	Yes	Down	10HDx	off
A8	10/100TX	No	Yes	Up	10FDx	off

Enables per-port flow control for ports A1 - A6.

Figure 10-8. Example of Configuring Flow Control for a Series of Ports

```
ProCurve(config)# no int a5-a6 flow-control
ProCurve(config)# show interfaces brief
Status and Counters - Port Status
```

Port	Type	Intrusion Alert	Enabled	Status	Mode	Flow Ctrl
A1	10/100TX	No	Yes	Down	10FDx	on
A2	10/100TX	No	Yes	Down	10FDx	on
A3	10/100TX	No	Yes	Down	10FDx	on
A4	10/100TX	No	Yes	Down	10FDx	on
A5	10/100TX	No	Yes	Down	10FDx	off
A6	10/100TX	No	Yes	Down	10FDx	off
A7	10/100TX	No	Yes	Up	10HDx	off
A8	10/100TX	No	Yes	Down	10FDx	off

Disables per-port flow control on ports A5 and A6.

Figure 10-9. Example Continued from Figure 10-8

```

ProCurve(config)# no int a1-a4 flow-control
ProCurve(config)# show interfaces brief
Status and Counters - Port Status

```

Port	Type	Intrusion Alert	Enabled	Status	Mode	Flow Ctrl
A1	10/100TX	No	Yes	Down	10FDx	off
A2	10/100TX	No	Yes	Down	10FDx	off
A3	10/100TX	No	Yes	Down	10FDx	off
A4	10/100TX	No	Yes	Down	10FDx	off
A5	10/100TX	No	Yes	Down	10FDx	off
A6	10/100TX	No	Yes	Down	10FDx	off
A7	10/100TX	No	Yes	Up	10HDx	off
A8	10/100TX	No	Yes	Down	10FDx	off
.						
.						
.						

Disables per-port flow control on ports A1 through A4. Flow control is now disabled on the switch.

Ports formerly configured for flow control.

Figure 10-10. Example Continued from Figure 10-9

Configuring a Broadcast Limit on the Switch

Broadcast-Limit on switches covered in this guide is configured on a per-port basis. You must be at the port context level for this command to work, for example:

```

ProCurve(config)#int B1
ProCurve(int B1)# broadcast-limit 1

```

Broadcast-Limit.

Syntax: broadcast-limit <0-99>

*Enables or disables broadcast limiting for outbound broadcasts on a selected port on the switch. The value selected is the percentage of traffic allowed, for example, **broadcast-limit 5** allows 5% of the maximum amount of traffic for that port. A value of zero disables broadcast limiting for that port.*

Note: You must switch to port context level before issuing the **broadcast-limit** command.

Note: This feature is not appropriate for networks requiring high levels of IPX or RIP broadcast traffic.

Syntax: show config

Displays the startup-config file. The broadcast limit setting appears here if enabled and saved to the startup-config file.

Syntax: show running-config

Displays the running-config file. The broadcast limit setting appears here if enabled. If the setting is not also saved to the startup-config file, rebooting the switch returns broadcast limit to the setting currently in the startup-config file.

For example, the following command enables broadcast limiting of 1 percent of the traffic rate on the selected port on the switch:

```
ProCurve(int B1)# broadcast-limit 1
```

For a one Gbps port this results in a broadcast traffic rate of ten Mbps.

Configuring ProCurve Auto-MDIX

Copper ports on the switch can automatically detect the type of cable configuration (MDI or MDI-X) on a connected device and adjust to operate appropriately.

This means you can use a “straight-through” twisted-pair cable or a “cross-over” twisted-pair cable for any of the connections—the port makes the necessary adjustments to accommodate either one for correct operation. The following port types on your switch support the IEEE 802.3ab standard, which includes the “Auto MDI/MDI-X” feature:

- 10/100-TX xl module ports
- 100/1000-T xl module ports
- 10/100/1000-T xl module ports

Using the above ports:

- If you connect a copper port using a straight-through cable on a switch to a port on another switch or hub that uses MDI-X ports, the switch port automatically operates as an MDI port.
- If you connect a copper port using a straight-through cable on a switch to a port on an end node, such as a server or PC, that uses MDI ports, the switch port automatically operates as an MDI-X port.

ProCurve Auto-MDIX was developed for auto-negotiating devices, and was shared with the IEEE for the development of the IEEE 802.3ab standard. ProCurve Auto-MDIX and the IEEE 802.3ab Auto MDI/MID-X feature are completely compatible. Additionally, ProCurve Auto-MDIX supports operation in forced speed and duplex modes.

If you want more information on this subject please refer to the *IEEE 802.3ab Standard Reference*.

For more information on MDI-X, refer to the appendix titled “Switch Ports and Network Cables” in the *Installation and Getting Started Guide* for your switch.

Manual Override. If you require control over the MDI/MDI-X feature you can set the switch to either of two non-default modes:

- Manual MDI
- Manual MDI-X

Table 10-2 shows the cabling requirements for the MDI/MDI-X settings.

Table 10-2. Cable Types for Auto and Manual MDI/MDI-X Settings

Setting	MDI/MDI-X Device Type	
	PC or Other MDI Device Type	Switch, Hub, or Other MDI-X Device
Manual MDI	Crossover Cable	Straight-Through Cable
Manual MDI-X	Straight-Through Cable	Crossover Cable
Auto-MDI-X (The Default)	Either Crossover or Straight-Through Cable	

The Auto-MDIX features apply only to copper port switches using twisted-pair copper Ethernet cables.

Syntax: interface < port-list > mdix-mode < auto-mdix | mdi | mdix >

auto-mdix is the automatic, default setting. This configures the port for automatic detection of the cable (either straight-through or crossover).

mdi is the manual mode setting that configures the port for connecting to either a PC or other MDI device with a crossover cable, or to a switch, hub, or other MDI-X device with a straight-through cable.

mdix is the manual mode setting that configures the port for connecting to either a switch, hub, or other MDI-X device with a crossover cable, or to a PC or other MDI device with a straight-through cable.

Syntax: show interfaces config

Lists the current per-port Auto/MDI/MDI-X configuration.

Syntax: show interfaces brief

Where a port is linked to another device, this command lists the MDI mode the port is currently using. In the case of ports configured for **Auto (auto-mdix)**, the MDI mode appears as either **MDI** or **MDIX**, depending upon which option the port has negotiated with the device on the other end of the link. In the case of ports configured for **MDI** or **MDIX**, the mode listed in this display matches the configured setting. If the link to another device was up, but has gone down, this command shows the last operating MDI mode the port was using. If a port on a given switch has not detected a link to another device since the last reboot, this command lists the MDI mode to which the port is currently configured.

For example, **show interfaces config** displays the following data when port A1 is configured for **auto-mdix**, port A2 is configured for **mdi**, and port A3 is configured for **mdix**.

```
ProCurve(config)# show interfaces config
```

Port Settings						Per-Port MDI Configuration
Port	Type	Enabled	Mode	Flow Ctrl	MDI	
A1	10/100TX	Yes	Auto	Disable	Auto	
A2	10/100TX	Yes	Auto	Disable	MDI	
A3	10/100TX	Yes	Auto	Disable	MDIX	
A4	10/100TX	Yes	Auto	Disable	Auto	
A5	10/100TX	Yes	Auto	Disable	Auto	
:	:	:	:	:	:	
:	:	:	:	:	:	

Figure 10-11. Example of Displaying the Current MDI Configuration

```
ProCurve(config)# show interfaces brief
```

Status and Counters - Port Status							Per-Port MDI Operating Mode
Port	Type	Intrusion Alert	Enabled	Status	Mode	MDI Mode	Flow Ctrl
A1	10/100TX	No	Yes	Up	100FDx	MDIX	off
A2	10/100TX	No	Yes	Up	100FDx	MDI	off
A3	10/100TX	No	Yes	Up	100FDx	MDIX	off
A4	10/100TX	No	Yes	Down	10FDx	Auto	off
A5	10/100TX	No	Yes	Down	10FDx	Auto	off
:	:	:	:	:	:	:	:
:	:	:	:	:	:	:	:

Figure 10-12. Example of Displaying the Current MDI Operating Mode

Web: Viewing Port Status and Configuring Port Parameters

In the web browser interface:

1. Click on the **Configuration** tab.
2. Click on **[Port Configuration]**.
3. Select the ports you want to modify and click on **[Modify Selected Ports]**.
4. After you make the desired changes, click on **[Apply Settings]**.

Note that the web browser interface displays an existing port trunk group. However, to configure a port trunk group, you must use the CLI or the menu interface. For more on this topic, refer to Chapter 11, “Port Trunking”.

Using Friendly (Optional) Port Names

Feature	Default	Menu	CLI	Web
Configure Friendly Port Names	Standard Port Numbering	n/a	page 20	n/a
Display Friendly Port Names	n/a	n/a	page 21	n/a

This feature enables you to assign alphanumeric port names of your choosing to augment automatically assigned numeric port names. This means you can configure meaningful port names to make it easier to identify the source of information listed by some **Show** commands. (Note that this feature *augments* port numbering, but *does not replace* it.)

Configuring and Operating Rules for Friendly Port Names

- At either the global or context configuration level you can assign a unique name to a port. You can also assign the same name to multiple ports.

- The friendly port names you configure appear in the output of the **show name [port-list]**, **show config**, and **show interface < port-number >** commands. They do not appear in the output of other show commands or in Menu interface screens. (Refer to “Displaying Friendly Port Names with Other Port Data” on page 10-21.)
- Friendly port names are not a substitute for port numbers in CLI commands or Menu displays.
- Trunking ports together does not affect friendly naming for the individual ports. (If you want the same name for all ports in a trunk, you must individually assign the name to each port.)
- A friendly port name can have up to 64 contiguous alphanumeric characters.
- Blank spaces within friendly port names are not allowed, and if used, cause an **invalid input** error. (The switch interprets a blank space as a name terminator.)
- In a port listing, **not assigned** indicates that the port does not have a name assignment other than its fixed port number.
- To retain friendly port names across reboots, you must save the current running-configuration to the startup-config file after entering the friendly port names. (In the CLI, use the **write memory** command.)

Configuring Friendly Port Names

Syntax: interface < port-list > name < port-name-string >
Assigns a port name to port-list.

Syntax: no interface < port-list > name
Deletes the port name from port-list.

Configuring a Single Port Name. Suppose that you have connected port A3 on the switch to Bill Smith’s workstation, and want to assign Bill’s name and workstation IP address (10.25.101.73) as a port name for port A3:

```
ProCurve(config)# int A3 name Bill_Smith@10.25.101.73
ProCurve(config)# write mem
ProCurve(config)# show name A3

Port Names
Port : A3
Type : 10/100TX
Name : Bill_Smith@10.25.101.73
```

Figure 10-13. Example of Configuring a Friendly Port Name

Configuring the Same Name for Multiple Ports. Suppose that you want to use ports A5 through A8 as a trunked link to a server used by a drafting group. In this case you might configure ports A5 through A8 with the name “Draft-Server:Trunk”.

```
ProCurve(config)# int A5-A8 name Draft-Server:Trunk
ProCurve(config)# write mem
ProCurve(config)# show name 5-8

Port Names

Port : A5
Type : 10/100TX
Name : Draft-Server:Trunk

Port : A6
Type : 10/100TX
Name : Draft-Server:Trunk

Port : A7
Type : 10/100TX
Name : Draft-Server:Trunk

Port : A8
Type : 10/100TX
Name : Draft-Server:Trunk
```

Figure 10-14. Example of Configuring One Friendly Port Name on Multiple Ports

Displaying Friendly Port Names with Other Port Data

You can display friendly port name data in the following combinations:

- **show name:** Displays a listing of port numbers with their corresponding friendly port names and also quickly shows you which ports do not have friendly name assignments. (**show name** data comes from the running-config file.)
- **show interface <port-number>:** Displays the friendly port name, if any, along with the traffic statistics for that port. (The friendly port name data comes from the running-config file.)
- **show config:** Includes friendly port names in the per-port data of the resulting configuration listing. (**show config** data comes from the startup-config file.)

To List All Ports or Selected Ports with Their Friendly Port Names.

This command lists names assigned to a specific port.

Syntax: show name [port-list]

*Lists the friendly port name with its corresponding port number and port type. The **show name** command without a port list shows this data for all ports on the switch.*

For example:

```
ProCurve(config)# show name
Port Names
Port Type      Name
-----
A1  10/100TX  not assigned
A2  10/100TX  not assigned
A3  10/100TX  Bill_Smith@10.25.101.73
A4  10/100TX  not assigned
A5  10/100TX  Draft-Server:Trunk
A6  10/100TX  Draft-Server:Trunk
A7  10/100TX  Draft-Server:Trunk
A8  10/100TX  Draft-Server:Trunk
A9  10/100TX  not assigned
A10 10/100TX  not assigned
A11 10/100TX  not assigned
A12 10/100TX  not assigned
:    :
:    :
```

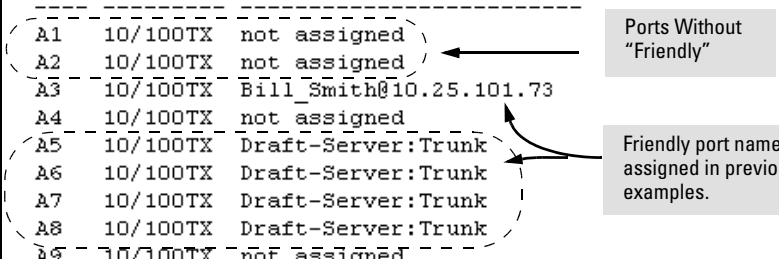


Figure 10-15. Example of Friendly Port Name Data for All Ports on the Switch

```
ProCurve(config)# show name A2,A3,A5
Port Names
Port : A2
Type : 10/100TX
Name : not assigned
Port : A3
Type : 10/100TX
Name : Bill_Smith@10.25.101.73
Port : A5
Type : 10/100TX
Name : Draft-Server:Trunk
```

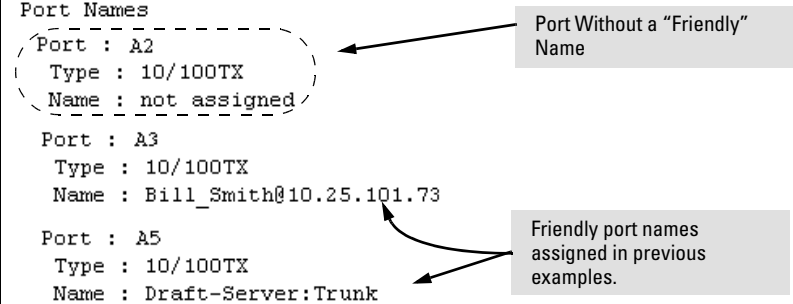


Figure 10-16. Example of Friendly Port Name Data for Specific Ports on the Switch

Including Friendly Port Names in Per-Port Statistics Listings. A friendly port name configured to a port is automatically included when you display the port's statistics output.

Syntax: show interface < port-number >

Includes the friendly port name with the port's traffic statistics listing.

For example, if you configure port A1 with the name "O'Connor_10.25.101.43", the show interface output for this port appears similar to the following:

```
ProCurve(config)# show interface A1
Status and Counters - Port Counters for port A1

Name      : O'Connor@10.25.101.43 ← Friendly Port Name
Link Status      : Up

Bytes Rx      : 894,568           Bytes Tx      : 2470
Unicast Rx    : 1179             Unicast Tx    : 13
Bcast/Mcast Rx : 5280           Bcast/Mcast Tx : 13

FCS Rx       : 36                Drops Tx      : 0
Alignment Rx : 2                Collisions Tx : 0
Runts Rx     : 0                Late Colln Tx : 0
Giants Rx    : 0                Excessive Colln : 0
Total Rx Errors : 38           Deferred Tx   : 0
```

Figure 10-17. Example of a Friendly Port Name in a Per-Port Statistics Listing

For a given port, if a friendly port name does not exist in the running-config file, the Name line in the above command output appears as:

```
Name      : not assigned
```

To Search the Configuration for Ports with Friendly Port Names.

This option tells you which friendly port names have been saved to the startup-config file. (**show config** does not include ports that have only default settings in the startup-config file.)

Syntax: show config

Includes friendly port names in a listing of all interfaces (ports) configured with non-default settings. Excludes ports that have neither a friendly port name nor any other non-default configuration settings.

Port Status and Configuration

Using Friendly (Optional) Port Names

For example, if you configure port A1 with a friendly port name:

```
ProCurve(config)# int A1 name Print_Server@10.25.101.43
ProCurve(config)# write mem
ProCurve(config)# int A2 name Herbert's PC
ProCurve(config)# show config

Startup configuration:
; J4850A Configuration Editor; Created on release #E.08.30
hostname "HPswitch"
time daylight-time-rule None
no cdp run
interface A1
  name "Print_Server@10.25.101.43"
exit
snmp-server community "public" Unrestricted
vlan 1
  name "DEFAULT_VLAN"
  untagged 1-24
  ip address dhcp-bootp
  exit
no aaa port-access authenticator active
```

This command sequence saves the friendly port name for port A1 in the startup-config file. The name entered for port A2 is not saved because it was executed after **write memory**.

Listing includes friendly port name for port A1 only.

In this case, **show config** lists only port A1. Executing **write mem** after entering the name for port A2, and then executing **show config** again would result in a listing that includes both ports.

Figure 10-18. Example Listing of the Startup-Config File with a Friendly Port Name Configured (and Saved)

Configuring Transceivers and Modules That Haven't Been Inserted

Transceivers

Previously, a port had to be valid and verified for the switch to allow it to be configured. Transceivers are removable ports and considered invalid when not present in the switch, so they cannot be configured unless they are already in the switch. For switches covered in this guide, the verification for allowable port configurations performed by the CLI is removed and configuration of transceivers is allowed even if they are not yet inserted in the switch.

Modules

You can create or edit configuration files (as text files) that can be uploaded to the switch without the modules having been installed yet. Additionally, you can pre-configure the modules with the CLI **module** command.

Syntax: module <module-num> type <module-type>

Allows you to configure the type of the module.

The same **module** command used in an uploaded configuration file is used to define a module that is being pre-configured. The validation performed when issued through the CLI is still performed just as if the command was executed on the switch, in other words, as if the module were actually present in the switch.

Note

You cannot use this method to change the configuration of a module that has already been configured. The slot must be empty and the configuration file must not have a configuration associated with it.

Uni-Directional Link Detection (UDLD)

Uni-directional Link Detection (UDLD) monitors a link between two ProCurve switches and blocks the ports on both ends of the link if the link fails at any point between the two devices. This feature is particularly useful for detecting failures in fiber links and trunks. Figure 10-19 shows an example.

Scenario 1 (No UDLD): Without UDLD, the switch ports remain enabled despite the link failure. Traffic continues to be load-balanced to the ports connected to the failed link.

Scenario 2 (UDLD-enabled): When UDLD is enabled, the feature blocks the ports connected to the failed link.

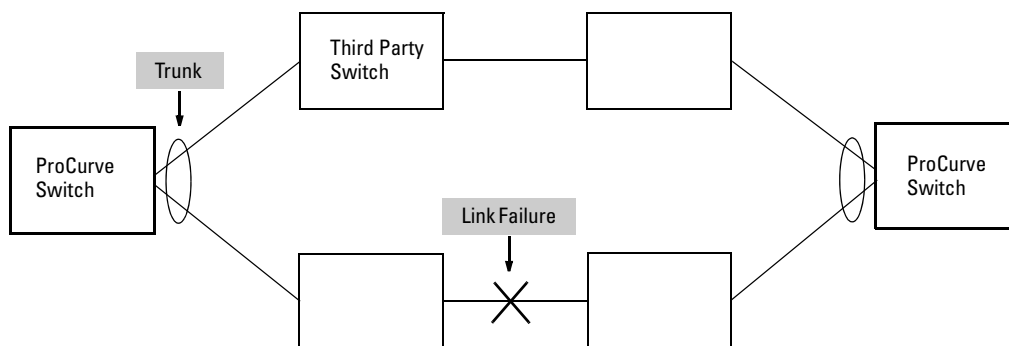


Figure 10-19. UDLD Example

In this example, each ProCurve switch load balances traffic across two ports in a trunk group. Without the UDLD feature, a link failure on a link that is not directly attached to one of the ProCurve switches remains undetected. As a result, each switch continues to send traffic on the ports connected to the failed link. When UDLD is enabled on the trunk ports on each ProCurve switch, the switches detect the failed link, block the ports connected to the failed link, and use the remaining ports in the trunk group to forward the traffic.

Similarly, UDLD is effective for monitoring fiber optic links that use two uni-direction fibers to transmit and receive packets. Without UDLD, if a fiber breaks in one direction, a fiber port may assume the link is still good (because the other direction is operating normally) and continue to send traffic on the

connected ports. UDLD-enabled ports; however, will prevent traffic from being sent across a bad link by blocking the ports in the event that either the individual transmitter or receiver for that connection fails.

Ports enabled for UDLD exchange health-check packets once every five seconds (the link-keepalive interval). If a port does not receive a health-check packet from the port at the other end of the link within the keepalive interval, the port waits for four more intervals. If the port still does not receive a health-check packet after waiting for five intervals, the port concludes that the link has failed and blocks the UDLD-enabled port.

When a port is blocked by UDLD, the event is recorded in the switch log or via an SNMP trap (if configured); and other port blocking protocols, like spanning tree, will not use the bad link to load balance packets. The port will remain blocked until the link is unplugged, disabled, or fixed. The port can also be unblocked by disabling UDLD on the port.

Configuring UDLD

When configuring UDLD, keep the following considerations in mind:

- UDLD is configured on a per-port basis and must be enabled at both ends of the link. See the note below for a list of ProCurve switches that support UDLD.
- To configure UDLD on a trunk group, you must configure the feature on each port of the group individually. Configuring UDLD on a trunk group's primary port enables the feature on that port only.
- Dynamic trunking is not supported. If you want to configure a trunk group that contains ports on which UDLD is enabled, you must remove the UDLD configuration from the ports. After you create the trunk group, you can re-add the UDLD configuration.

Note

UDLD interoperates with the following ProCurve switch series: 2600, 2800, 2900, 3400, 3500, 4200, 5300, 5400, 6200, 6400, 8212, and 9300. Consult the release notes and current manuals for required software versions.

The following commands allow you to configure UDLD via the CLI.

Syntax: [no] interface <port-list> link-keepalive

Enables UDLD on a port or range of ports.

*To disable the feature, enter the **no** form of the command.*

Default: UDLD disabled

Syntax: link-keepalive interval <interval>

Determines the time interval to send UDLD control packets. The <interval> parameter specifies how often the ports send a UDLD packet. You can specify from 10 – 100, in 100 ms increments, where 10 is 1 second, 11 is 1.1 seconds, and so on.

Default: 50 (5 seconds)

Syntax: link-keepalive retries <num>

Determines the maximum number of retries to send UDLD control packets. The <num> parameter specifies the maximum number of times the port will try the health check. You can specify a value from 3 – 10.

Default: 5

Syntax: [no] interface <port-list> link-keepalive vlan <vid>

Assigns a VLAN ID to a UDLD-enabled port for sending of tagged UDLD control packets. Under default settings, untagged UDLD packets can still be transmitted and received on tagged only ports—however, a warning message will be logged.

*The **no** form of the command disables UDLD on the specified port(s).*

Default: UDLD packets are untagged; tagged only ports will transmit and receive untagged UDLD control packets

Enabling UDLD

UDLD is enabled on a per port basis. For example, to enable UDLD on port a1, enter:

```
ProCurve(config)#interface a1 link-keepalive
```

To enable the feature on a trunk group, enter the appropriate port range. For example:

```
ProCurve(config)#interface a1-a4 link-keepalive
```

Note

When at least one port is UDLD-enabled, the switch will forward out UDLD packets that arrive on non-UDLD-configured ports out of all other non-UDLD-configured ports in the same vlan. That is, UDLD control packets will “pass through” a port that is not configured for UDLD. However, UDLD packets will be dropped on any blocked ports that are not configured for UDLD.

Changing the Keepalive Interval

By default, ports enabled for UDLD send a link health-check packet once every 5 seconds. You can change the interval to a value from 10 – 100 deciseconds, where 10 is 1 second, 11 is 1.1 seconds, and so on. For example, to change the packet interval to seven seconds, enter the following command at the global configuration level:

```
ProCurve(config)# link-keepalive interval 70
```

Changing the Keepalive Retries

By default, a port waits five seconds to receive a health-check reply packet from the port at the other end of the link. If the port does not receive a reply, the port tries four more times by sending up to four more health-check packets. If the port still does not receive a reply after the maximum number of retries, the port goes down.

You can change the maximum number of keepalive attempts to a value from 3 – 10. For example, to change the maximum number of attempts to 4, enter the following command at the global configuration level:

```
ProCurve(config)# link-keepalive retries 4
```

Configuring UDLD for Tagged Ports

The default implementation of UDLD sends the UDLD control packets untagged, even across tagged ports. If an untagged UDLD packet is received by a non-ProCurve switch, that switch may reject the packet. To avoid such an occurrence, you can configure ports to send out UDLD control packets that are tagged with a specified VLAN.

To enable ports to receive and send UDLD control packets tagged with a specific VLAN ID, enter a command such as the following at the interface configuration level:

```
ProCurve(config)#interface 1 link-keepalive vlan 22
```

Notes

- You must configure the same VLANs that will be used for UDLD on all devices across the network; otherwise, the UDLD link cannot be maintained.
- If a VLAN ID is not specified, then UDLD control packets are sent out of the port as untagged packets.

- To re-assign a VLAN ID, re-enter the command with the new VLAN ID number. The new command will overwrite the previous command setting.
- When configuring UDLD for tagged ports, you may receive a warning message if there are any inconsistencies with the port's VLAN configuration (see page 32 for potential problems).

Viewing UDLD Information

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

Syntax: show link-keepalive

Displays all the ports that are enabled for link-keepalive.

Syntax: show link-keepalive statistics

Displays detailed statistics for the UDLD-enabled ports on the switch.

Syntax: clear link-keepalive statistics

Clears UDLD statistics. This command clears the packets sent, packets received, and transitions counters in the show link-keepalive statistics display.

To display summary information on all UDLD-enabled ports, enter the **show link-keepalive** command. For example:

```
ProCurve(config)# show link-keepalive

Total link-keepalive enabled ports: 4
Keepalive Retries: 3           Keepalive Interval: 1 sec

Port Enabled Physical  Keepalive  Adjacent  UDLD
      Status   Status    Status    Switch    VLAN
-----
1  Yes   up       up        00d9d-f9b700  200
2  Yes   up       up        01560-7b1600
3  Yes   down    off-line
4  Yes   up       failure
5  No    down    off-line
```

Figure 10-20. Example of Show Link-Keepalive Command

To display detailed UDLD information for specific ports, enter the **show link-keepalive statistics** command. For example:

```
ProCurve(config)# show link-keepalive statistics
```

Port:	1		
Current State:	up	Neighbor MAC Addr:	0000a1-b1c1d1
Uddl Packets Sent:	1000	Neighbor Port:	5
Uddl Packets Received:	1000	State Transitions:	2
Port Blocking:	no	Link-vlan:	1
Port:	2		
Current State:	up	Neighbor MAC Addr:	000102-030405
Uddl Packets Sent:	500	Neighbor Port:	6
Uddl Packets Received:	450	State Transitions:	3
Port Blocking:	no	Link-vlan:	200
Port:	3		
Current State:	off line	Neighbor MAC Addr:	n/a
Uddl Packets Sent:	0	Neighbor Port:	n/a
Uddl Packets Received:	0	State Transitions:	0
Port Blocking:	no	Link-vlan:	1
Port:	4		
Current State:	failure	Neighbor MAC Addr:	n/a
Uddl Packets Sent:	128	Neighbor Port:	n/a
Uddl Packets Received:	50	State Transitions:	8
Port Blocking:	yes	Link-vlan:	1

Ports 1 and 2 are UDLD-enabled and show the number of health check packets sent and received on each port.

Port 4 is shown as blocked due to a link-keepalive failure

Figure 10-21. Example of Show Link-Keepalive Statistics Command

To clear UDLD statistics, enter the following command:

```
ProCurve# clear link-keepalive statistics
```

This command clears the packets sent, packets received, and transitions counters in the **show link keepalive statistics** display (see Figure 10-21 for an example).

Configuration Warnings and Event Log Messages

Warning Messages. The following table shows the warning messages that may be issued and their possible causes, when UDLD is configured for tagged ports.

Table 10-3. Warning Messages caused by configuring UDLD for Tagged Ports

CLI Command Example	Warning Message	Possible Problem
link-keepalive 6	Possible configuration problem detected on port 6. UDLD VLAN configuration does not match the port's VLAN configuration.	You have attempted to enable UDLD on a port that is a tagged only port, but did not specify a configuration for tagged UDLD control packets. In this example, the switch will send and receive the UDLD control packets untagged despite issuing this warning.
link-keepalive 7 vlan 4	Possible configuration problem detected on port 7. UDLD VLAN configuration does not match the port's VLAN configuration.	You have attempted to configure tagged UDLD packets on a port that does not belong to the specified VLAN. In this example, if port 7 belongs to VLAN 1 and 22, but the user tries to configure UDLD on port 7 to send tagged packets in VLAN 4, the configuration will be accepted. The UDLD control packets will be sent tagged in VLAN 4, which may result in the port being blocked by UDLD if the user does not configure VLAN 4 on this port.
no vlan 22 tagged 20	Possible configuration problem detected on port 18. UDLD VLAN configuration does not match the port's VLAN configuration.	You have attempted to remove a VLAN on port that is configured for tagged UDLD packets on that VLAN. In this example, if port 18, 19, and 20 are transmitting and receiving tagged UDLD packets for Vlan 22, but the user tries to remove Vlan 22 on port 20, the configuration will be accepted. In this case, the UDLD packets will still be sent on Vlan 20, which may result in the port being blocked by UDLD if the users do not change the UDLD configuration on this port.

Note: If you are configuring the switch via SNMP with the same problematic VLAN configuration choices, the above warning messages will also be logged in the switch's event log.

Event Log Messages. The following table shows the event log messages that may be generated once UDLD has been enabled on a port.

Table 10-4. UDLD Event Log Messages

Message	Event
I 01/01/06 04:25:05 ports: port 4 is deactivated due to link failure.	A UDLD-enabled port has been blocked due to part of the link having failed.
I 01/01/06 06:00:43 ports: port 4 is up, link status is good.	A failed link has been repaired and the UDLD-enabled port is no longer blocked.