Monitoring and Analyzing Switch Operation

Contents

Overview

The switches covered in this guide have several built-in tools for monitoring, analyzing, and troubleshooting switch and network operation:

- **Status:** Includes options for displaying general switch information, management address data, port status, port and trunk group statistics, MAC addresses detected on each port or VLAN, and STP, IGMP, and VLAN data (page B-5).
- **Counters:** Display details of traffic volume on individual ports (page B-14).
- **Event Log**: Lists switch operating events *(*"Using the Event Log for Troubleshooting Switch Problems" on page C-27*)*.
- **Alert Log:** Lists network occurrences detected by the switch—in the Status | Overview screen of the web browser interface (page 5-20).
- **Configurable trap receivers:** Uses SNMP to enable management stations on your network to receive SNMP traps from the switch. (Refer to "SNMPv1 and SNMPv2c Traps" on page 14-19.)
- **Port monitoring (mirroring):** Copy all traffic from the specified ports to a designated monitoring port (page B-26).

Note

Link test and ping test—analysis tools in troubleshooting situations—are described in Appendix C, "Troubleshooting". Refer to "Diagnostic Tools" on page C-59.

Status and Counters Data

This section describes the status and counters screens available through the switch console interface and/or the web browser interface.

Note

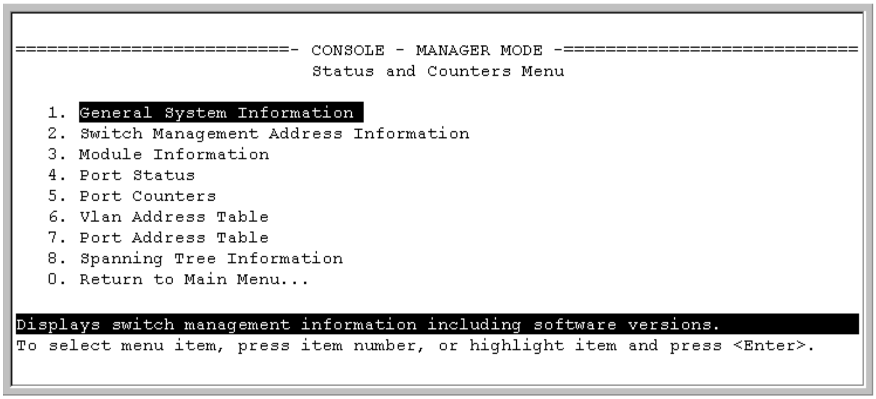
You can access all console screens from the web browser interface via Telnet to the console. Telnet access to the switch is available in the Device View window under the **Configuration** tab.

Status or Counters Type	Interface	Purpose	Page
Menu Access to Status and Counters	Menu	Access menu interface for status and counter data.	**B-6**
General System Information	Menu, CLI	Lists switch-level operating information.	**B-7**
Management Address Information	Menu, CLI	Lists the MAC address, IP address, and IPX network number for each VLAN or, if no VLANs are configured, for the switch.	**B-9**
Module Information	Menu, CLI	Lists the module type and description for each slot in which a module is installed.	**B-11**
Port Status	Menu, CLI, Web	Displays the operational status of each port.	**B-13**
Port and Trunk Statistics and Flow Control Status	Menu, CLI, Web	Summarizes port activity and lists per-port flow control status.	**B-14**
VLAN Address Table	Menu, CLI	Lists the MAC addresses of nodes the switch has detected on specific VLANs, with the corresponding switch port.	**B-17**
Port Address Table	Menu, CLI	Lists the MAC addresses that the switch has learned from the selected port.	**B-17**
STP Information	Menu, CLI	Lists Spanning Tree Protocol data for the switch and for individual ports. If VLANs are configured, reports on a per-VLAN basis.	**B-21**
IGMP Status	Menu, CLI	Lists IGMP groups, reports, queries, and port on which querier is located.	**B-22**
VLAN Information	Menu, CLI	For each VLAN configured in the switch, lists 802.1Q VLAN ID and up/down status.	**B-23**
Port Status Overview and Port Counters	Web	Shows port utilization and counters, and the Alert Log.	**B-25**

Menu Access To Status and Counters

Beginning at the Main Menu, display the Status and Counters menu by selecting:

1. Status and Counters



```
==========================- CONSOLE - MANAGER MODE -===========================
                           Status and Counters Menu

   1. General System Information
   2. Switch Management Address Information
   3. Module Information
   4. Port Status
   5. Port Counters
   6. Vlan Address Table
   7. Port Address Table
   8. Spanning Tree Information
   0. Return to Main Menu...

Displays switch management information including software versions.
To select menu item, press item number, or highlight item and press <Enter>.
```

Figure B-1. The Status and Counters Menu

Each of the above menu items accesses the read-only screens described on the following pages. Refer to the online help for a description of the entries displayed in these screens.

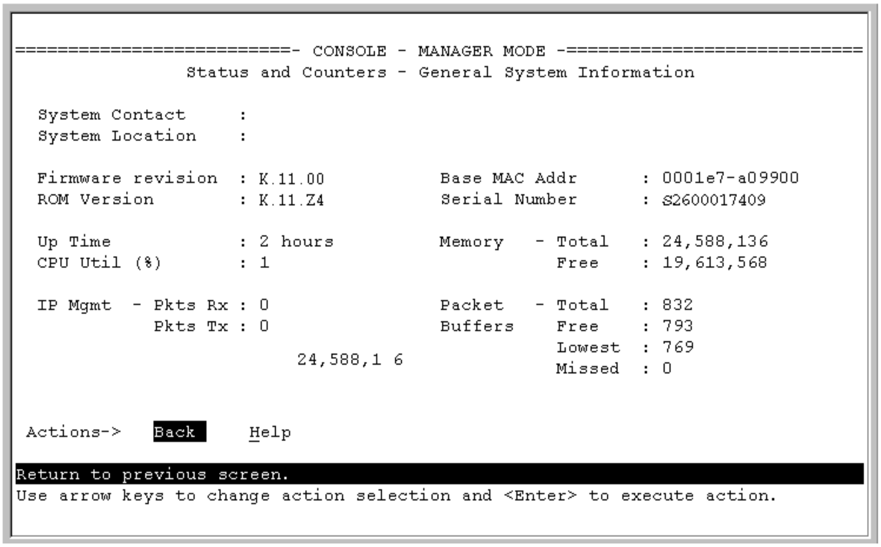
General System Information

Menu Access

From the console Main Menu, select:

1. Status and Counters

1. General System Information



```
=========================- CONSOLE - MANAGER MODE -===========================
                Status and Counters - General System Information

  System Contact     :
  System Location    :

  Firmware revision  : K.11.00          Base MAC Addr      : 0001e7-a09900
  ROM Version        : K.11.Z4          Serial Number      : S2600017409

  Up Time            : 2 hours          Memory   - Total   : 24,588,136
  CPU Util (%)       : 1                           Free    : 19,613,568

  IP Mgmt  - Pkts Rx : 0                Packet   - Total   : 832
             Pkts Tx : 0                Buffers    Free    : 793
                                                   Lowest  : 769
                          24,588,1 6               Missed  : 0


 Actions->   Back     Help

Return to previous screen.
Use arrow keys to change action selection and <Enter> to execute action.
```

Figure B-2. Example of General Switch Information

This screen dynamically indicates how individual switch resources are being used. Refer to the online Help for details.

CLI Access to System Information

The **show system** command displays general system information about the switch.

Syntax: show system [information | power-supply | temperature | fans]

Displays global system information and operational parameters for the switch.

information

Displays global system information and operational parameters for the switch.

power-supply

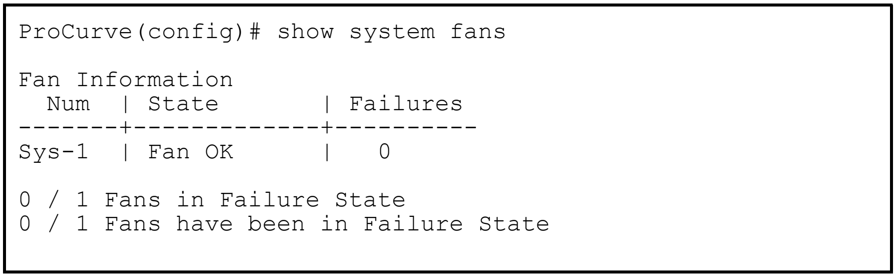
Shows chassis power supply and settings.

temperature

Shows system temperature and settings.

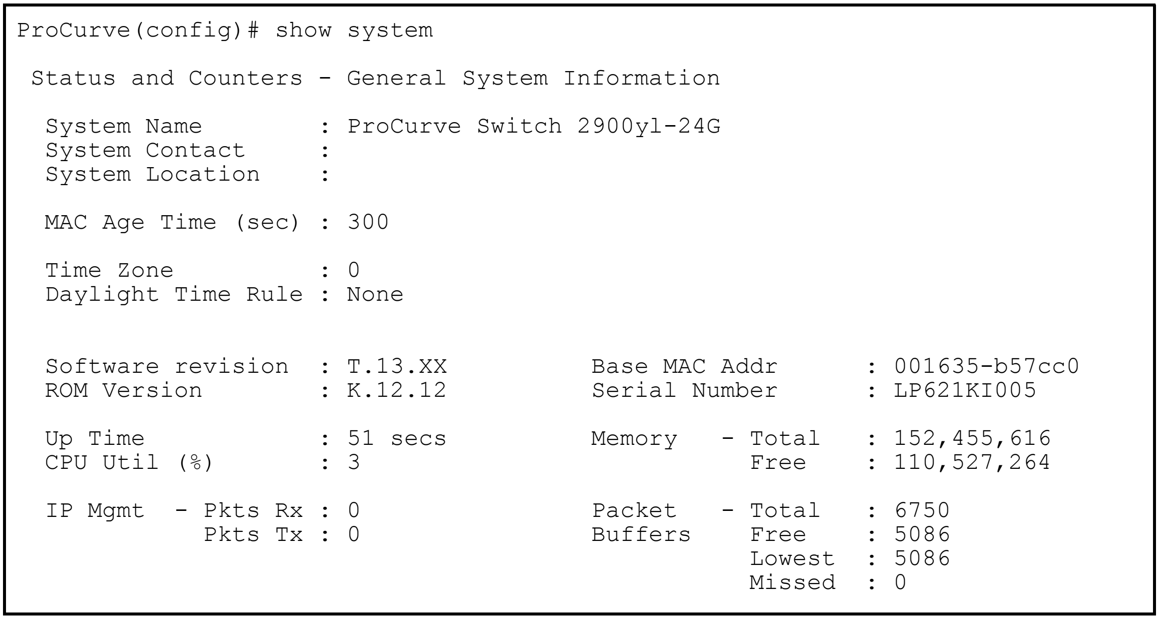
fans

Shows system fan status.



```
ProCurve(config)# show system fans

Fan Information
  Num  | State       | Failures
-------+-------------+----------
Sys-1  | Fan OK      |   0

0 / 1 Fans in Failure State
0 / 1 Fans have been in Failure State
```

Figure B-3. Example of System Fan Status



```
ProCurve(config)# show system

 Status and Counters - General System Information

  System Name         : ProCurve Switch 2900yl-24G
  System Contact      :
  System Location     :

  MAC Age Time (sec) : 300

  Time Zone           : 0
  Daylight Time Rule : None


  Software revision  : T.13.XX          Base MAC Addr      : 001635-b57cc0
  ROM Version         : K.12.12          Serial Number      : LP621KI005

  Up Time             : 51 secs          Memory   - Total    : 152,455,616
  CPU Util (%)        : 3                           Free     : 110,527,264

  IP Mgmt  - Pkts Rx : 0                Packet   - Total    : 6750
             Pkts Tx : 0                Buffers    Free     : 5086
                                                   Lowest   : 5086
                                                   Missed   : 0
```

Figure B-4. Example of Switch System Information

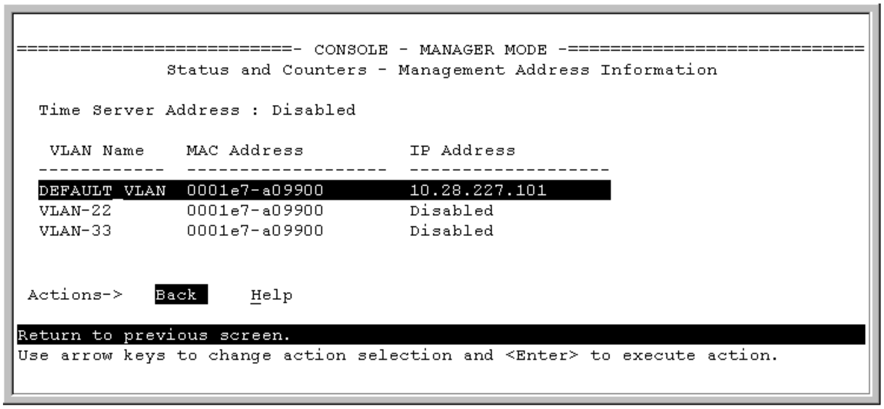
Switch Management Address Information

Menu Access

From the Main Menu, select:

1 Status and Counters . . .

2. Switch Management Address Information



```
==========================- CONSOLE - MANAGER MODE -============================
              Status and Counters - Management Address Information

  Time Server Address : Disabled

   VLAN Name    MAC Address          IP Address
  ------------ -------------------  --------------------
  DEFAULT_VLAN  0001e7-a09900        10.28.227.101
  VLAN-22       0001e7-a09900        Disabled
  VLAN-33       0001e7-a09900        Disabled


 Actions->   Back    Help

Return to previous screen.
Use arrow keys to change action selection and <Enter> to execute action.
```

Figure B-5. Example of Management Address Information with VLANs Configured

This screen displays addresses that are important for management of the switch. If multiple VLANs are *not* configured, this screen displays a single IP address for the entire switch. Refer to the online Help for details.

Note

As shown in figure B-5, all VLANs on the switches use the same MAC address. (This includes both the statically configured VLANs and any dynamic VLANs existing on the switch as a result of GVRP operation.)

Also, the switches covered in this guide use a multiple forwarding database. When using multiple VLANs and connecting a switch to a device that uses a single forwarding database, such as a Switch 4000M, there are cabling and tagged port VLAN requirements. For more on this topic, refer to the section titled “Multiple VLAN Considerations” in the “Static Virtual LANs (VLANs) chapter of the *Advanced Traffic Management Guide* for your switch.

CLI Access

Syntax: show management

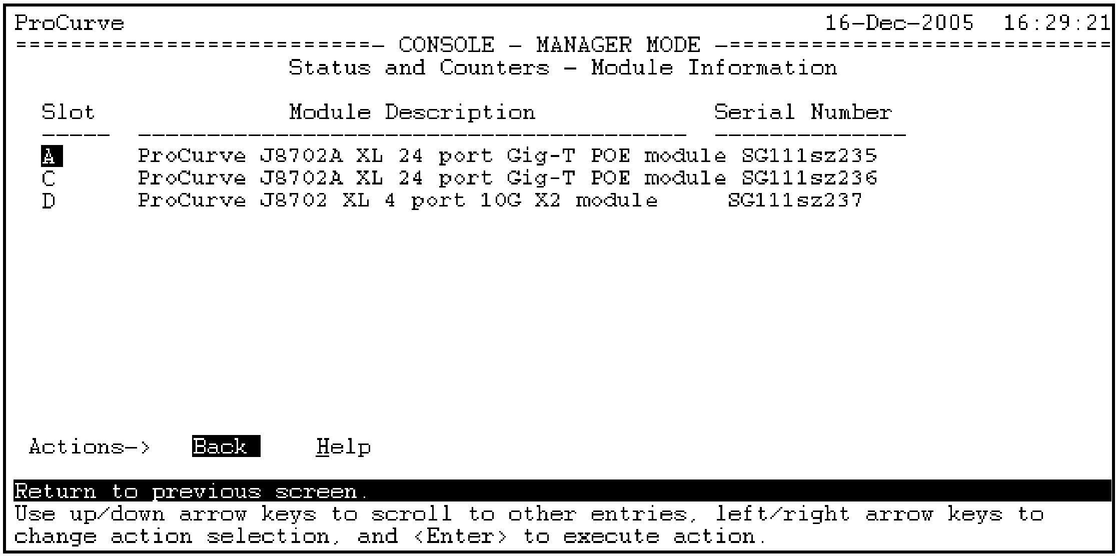
Module Information

Use this feature to determine which slots have modules installed and which type(s) of modules are installed.

Menu: Displaying Port Status

From the Main Menu, select:

1. Status and Counters ...
3. Module Information

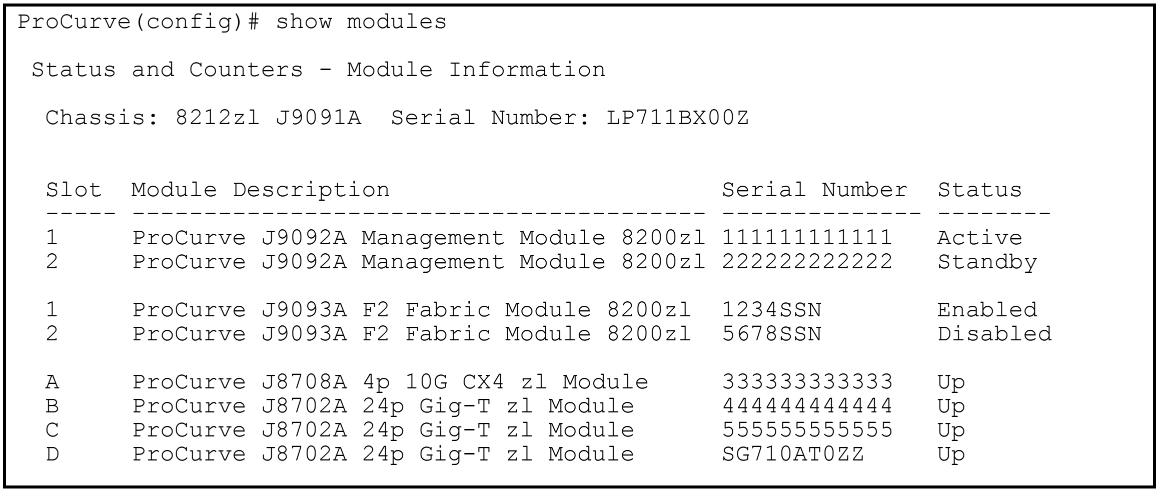


```
ProCurve                                                       16-Dec-2005  16:29:21
==========================- CONSOLE - MANAGER MODE -============================
                    Status and Counters - Module Information

  Slot             Module Description            Serial Number
  -----  ----------------------------------------  -------------
  A      ProCurve J8702A XL 24 port Gig-T POE module SG111sz235
  C      ProCurve J8702A XL 24 port Gig-T POE module SG111sz236
  D      ProCurve J8702 XL 4 port 10G X2 module     SG111sz237









 Actions->   Back     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.
```

Figure B-6. Example of Module Information in the Menu Interface

CLI Access

Syntax: show modules



```
ProCurve(config)# show modules

 Status and Counters - Module Information

  Chassis: 8212zl J9091A  Serial Number: LP711BX00Z


  Slot  Module Description                       Serial Number  Status
  ----- ---------------------------------------- -------------- --------
  1     ProCurve J9092A Management Module 8200zl 111111111111   Active
  2     ProCurve J9092A Management Module 8200zl 222222222222   Standby

  1     ProCurve J9093A F2 Fabric Module 8200zl  1234SSN        Enabled
  2     ProCurve J9093A F2 Fabric Module 8200zl  5678SSN        Disabled

  A     ProCurve J8708A 4p 10G CX4 zl Module     333333333333   Up
  B     ProCurve J8702A 24p Gig-T zl Module      444444444444   Up
  C     ProCurve J8702A 24p Gig-T zl Module      555555555555   Up
  D     ProCurve J8702A 24p Gig-T zl Module      SG710AT0ZZ     Up
```

Figure B-7. Example of Show Modules Command on an 8200zl Series Switch

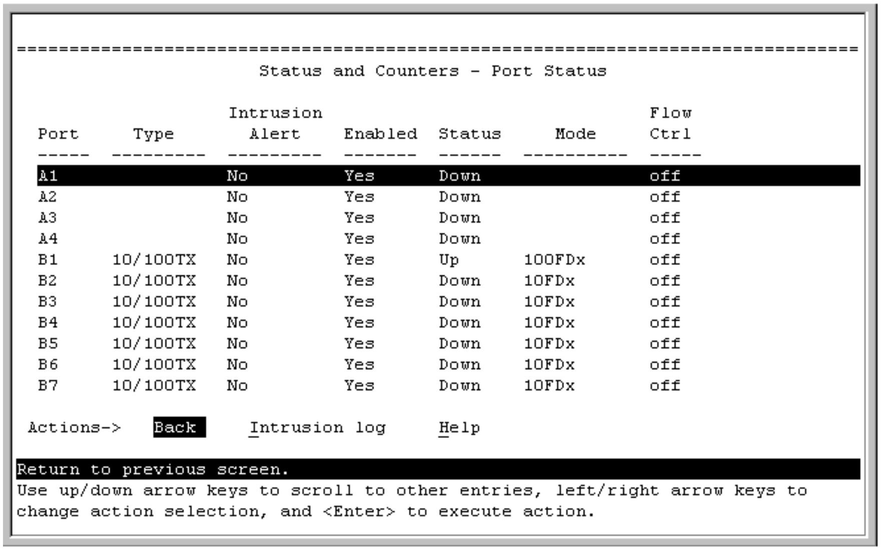
Port Status

The web browser interface and the console interface show the same port status data.

Menu: Displaying Port Status

From the Main Menu, select:

1. Status and Counters ...
4. Port Status



```
===============================================================================
                    Status and Counters - Port Status

                       Intrusion                                   Flow
  Port     Type          Alert     Enabled  Status      Mode       Ctrl
  -----  ---------   ---------   -------  ------  ----------   -----
  A1                   No          Yes      Down                   off
  A2                   No          Yes      Down                   off
  A3                   No          Yes      Down                   off
  A4                   No          Yes      Down                   off
  B1     10/100TX      No          Yes      Up      100FDx         off
  B2     10/100TX      No          Yes      Down    10FDx          off
  B3     10/100TX      No          Yes      Down    10FDx          off
  B4     10/100TX      No          Yes      Down    10FDx          off
  B5     10/100TX      No          Yes      Down    10FDx          off
  B6     10/100TX      No          Yes      Down    10FDx          off
  B7     10/100TX      No          Yes      Down    10FDx          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.
```

Figure B-8. Example of Port Status on the Menu Interface

CLI Access

Syntax: show interfaces brief

Web Access

1. Click on the **Status** tab.
2. Click on **[Port Status]**.

Viewing Port and Trunk Group Statistics and Flow Control Status

Feature	Default	Menu	CLI	Web
viewing port and trunk statistics for all ports, and flow control status	n/a	page B-15	page B-16	page B-16
viewing a detailed summary for a particular port or trunk	n/a	page B-15	page B-16	page B-16
resetting counters	n/a	page B-15	page B-16	page B-16

These features enable you to determine the traffic patterns for each port since the last reboot or reset of the switch. You can display:

- A general report of traffic on all LAN ports and trunk groups in the switch, along with the per-port flow control status (On or Off).
- A detailed summary of traffic on a selected port or trunk group.

You can also reset the counters for a specific port.

The menu interface and the web browser interface provide a dynamic display of counters summarizing the traffic on each port. The CLI lets you see a static "snapshot" of port or trunk group statistics at a particular moment.

As mentioned above, rebooting or resetting the switch resets the counters to zero. You can also reset the counters to zero for the current session. This is useful for troubleshooting. Refer to the "Note On Reset", below.

Note on Reset

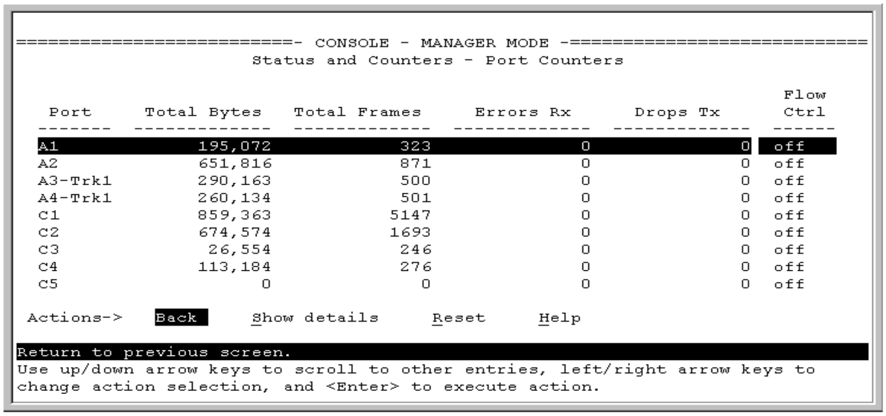
The **Reset** action resets the counter display to zero for the current session, but does not affect the cumulative values in the actual hardware counters. (In compliance with the SNMP standard, the values in the hardware counters are not reset to zero unless you reboot the switch.) Thus, using the **Reset** action resets the displayed counters to zero for the current session only. Exiting from the console session and starting a new session restores the counter displays to the accumulated values in the hardware counters.

Menu Access to Port and Trunk Statistics

To access this screen from the Main Menu, select:

1. Status and Counters …

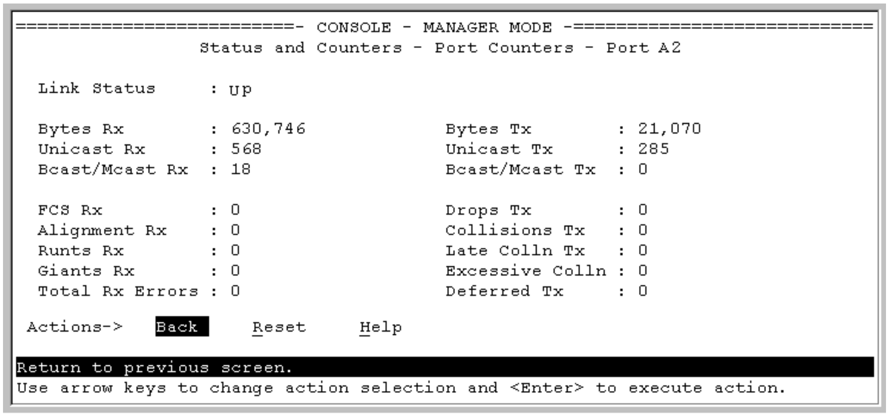
4. Port Counters



```
==========================- CONSOLE - MANAGER MODE -============================
                     Status and Counters - Port Counters

                                                                     Flow
  Port      Total Bytes   Total Frames    Errors Rx     Drops Tx     Ctrl
  -------  -------------  -------------  -------------  -------------  ------
  A1             195,072            323              0             0  off
  A2             651,816            871              0             0  off
  A3-Trk1        290,163            500              0             0  off
  A4-Trk1        260,134            501              0             0  off
  C1             859,363           5147              0             0  off
  C2             674,574           1693              0             0  off
  C3              26,554            246              0             0  off
  C4             113,184            276              0             0  off
  C5                   0              0              0             0  off

 Actions->   Back     Show details     Reset     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.
```

Figure B-9. Example of Port Counters on the Menu Interface

To view details about the traffic on a particular port, use the ↓ key to highlight that port number, then select **Show Details**. For example, selecting port A2 displays a screen similar to figure B-10, below.



```
==========================- CONSOLE - MANAGER MODE -============================
                  Status and Counters - Port Counters - Port A2

  Link Status      : Up

  Bytes Rx         : 630,746              Bytes Tx         : 21,070
  Unicast Rx       : 568                  Unicast Tx       : 285
  Bcast/Mcast Rx   : 18                   Bcast/Mcast Tx   : 0

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

 Actions->   Back     Reset     Help

Return to previous screen.
Use arrow keys to change action selection and <Enter> to execute action.
```

Figure B-10. Example of the Display for Show details on a Selected Port

This screen also includes the **Reset** action for the current session. (Refer to the “Note on Reset” on page B-14.)

CLI Access To Port and Trunk Group Statistics

To Display the Port Counter Summary Report.

Syntax: show interfaces

This command provides an overview of port activity for all ports on the switch.

To Display a Detailed Traffic Summary for Specific Ports. .

Syntax: show interfaces < *port-list* >

This command provides traffic details for the port(s) you specify

To Reset the Port Counters for a Specific Port.

Syntax: clear statistics < *port-list* >

This command resets the counters for the specified ports to zero for the current session. (See the "Note on Reset" on page B-14.)

Web Browser Access To View Port and Trunk Group Statistics

1. Click on the **Status** tab.
2. Click on **[Port Counters]**.
3. To refresh the counters for a specific port, click anywhere in the row for that port, then click on **[Refresh]**.

Note To reset the port counters to zero, you must reboot the switch.

Viewing the Switch's MAC Address Tables

Feature	Default	Menu	CLI	Web
viewing MAC addresses on all ports on a specific VLAN	n/a	page B-17	page B-20	—
viewing MAC addresses on a specific port	n/a	page B-19	page B-20	—
searching for a MAC address	n/a	page B-19	page B-20	—

These features help you to view:

- The MAC addresses that the switch has learned from network devices attached to the switch
- The port on which each MAC address was learned

Menu Access to the MAC Address Views and Searches

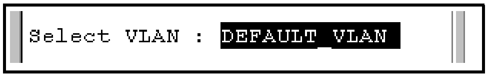
Per-VLAN MAC-Address Viewing and Searching. This feature lets you determine which switch port on a selected VLAN is being used to communicate with a specific device on the network. The per-VLAN listing includes:

- The MAC addresses that the switch has learned from network devices attached to the switch
- The port on which each MAC address was learned

1. From the Main Menu, select:

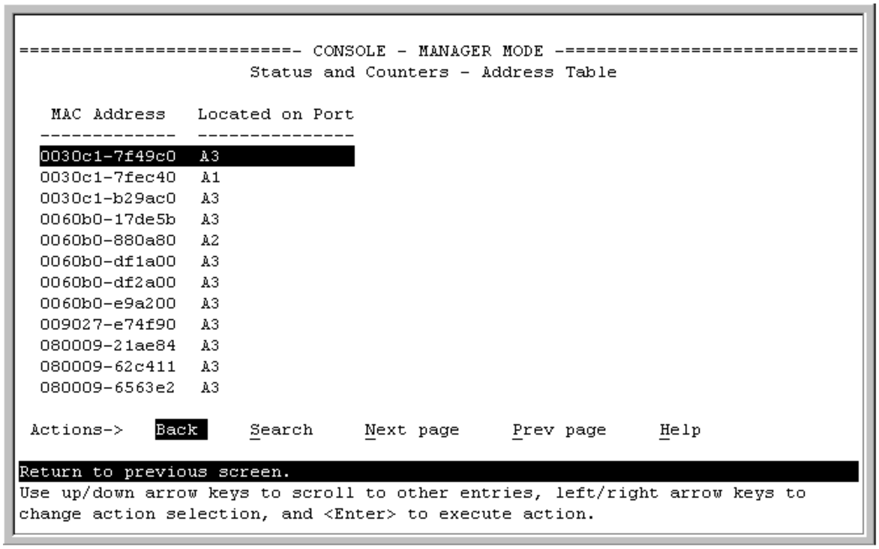
   1. Status and Counters
   5. VLAN Address Table

2. The switch then prompts you to select a VLAN.



```
Select VLAN : DEFAULT_VLAN
```

3. Use the Space bar to select the VLAN you want, then press **[Enter]**. The switch then displays the MAC address table for that VLAN:



```
==========================- CONSOLE - MANAGER MODE -============================
                       Status and Counters - Address Table

   MAC Address    Located on Port
  -------------  ---------------
  0030c1-7f49c0  A3
  0030c1-7fec40  A1
  0030c1-b29ac0  A3
  0060b0-17de5b  A3
  0060b0-880a80  A2
  0060b0-df1a00  A3
  0060b0-df2a00  A3
  0060b0-e9a200  A3
  009027-e74f90  A3
  080009-21ae84  A3
  080009-62c411  A3
  080009-6563e2  A3

 Actions->   Back    Search    Next page    Prev page    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.
```

Figure B-11. Example of the Address Table

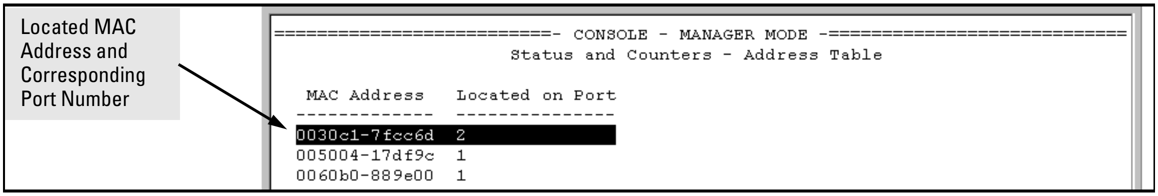
To page through the listing, use **Next page** and **Prev page**.

Finding the Port Connection for a Specific Device on a VLAN. This feature uses a device's MAC address that you enter to identify the port used by that device.

1. Proceeding from figure B-11, press **[S]** (for **Search**), to display the following prompt:

   ```
   Enter MAC address: _
   ```

2. Type the MAC address you want to locate and press **[Enter]**. The address and port number are highlighted if found. If the switch does not find the MAC address on the currently selected VLAN, it leaves the MAC address listing empty.



Located MAC Address and Corresponding Port Number

```
==========================- CONSOLE - MANAGER MODE -============================
                       Status and Counters - Address Table

  MAC Address    Located on Port
 -------------  ---------------
 0030c1-7fcc6d  2
 005004-17df9c  1
 0060b0-889e00  1
```

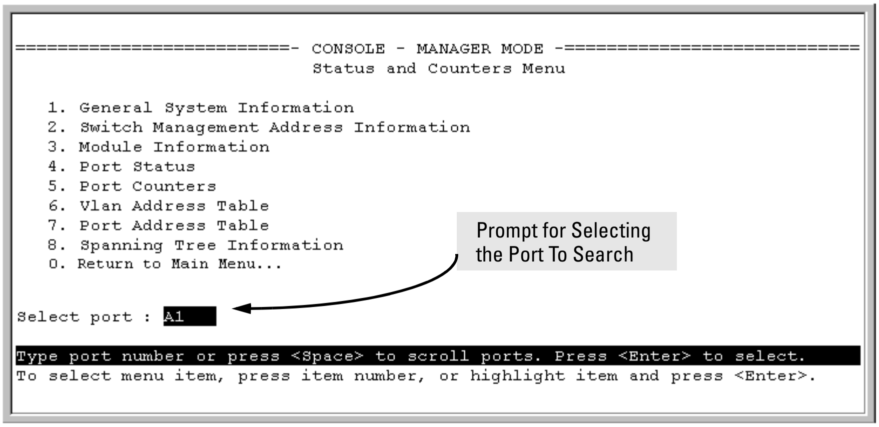
Figure B-12. Example of Menu Indicating Located MAC Address

3. Press **[P]** (for **Prev page**) to return to the full address table listing.

Port-Level MAC Address Viewing and Searching. This feature displays and searches for MAC addresses on the specified port instead of for all ports on the switch.

1. From the Main Menu, select:

   1. Status and Counters
   7. Port Address Table



```
==========================- CONSOLE - MANAGER MODE -============================
                            Status and Counters Menu

   1. General System Information
   2. Switch Management Address Information
   3. Module Information
   4. Port Status
   5. Port Counters
   6. Vlan Address Table
   7. Port Address Table
   8. Spanning Tree Information
   0. Return to Main Menu...

Select port : A1

Type port number or press <Space> to scroll ports. Press <Enter> to select.
To select menu item, press item number, or highlight item and press <Enter>.
```

Figure B-13. Listing MAC Addresses for a Specific Port

2. Use the Space bar to select the port you want to list or search for MAC addresses, then press **[Enter]** to list the MAC addresses detected on that port.

Determining Whether a Specific Device Is Connected to the Selected Port. Proceeding from step 2, above:

1. Press **[S]** (for **Search**), to display the following prompt:

   `Enter MAC address: _`

2. Type the MAC address you want to locate and press **[Enter]**. The address is highlighted if found. If the switch does not find the address, it leaves the MAC address listing empty.

3. Press **[P]** (for **Prev page**) to return to the previous per-port listing.

CLI Access for MAC Address Views and Searches

Syntax: show mac-address
[vlan < *vlan-id* >]
[< *port-list* >]
[< mac-addr >]

To List All Learned MAC Addresses on the Switch, with The Port Number on Which Each MAC Address Was Learned.

ProCurve> show mac-address

To List All Learned MAC Addresses on one or more ports, with Their Corresponding Port Numbers. For example, to list the learned MAC address on ports A1 through A4 and port A6:

ProCurve> show mac-address a1-a4,a6

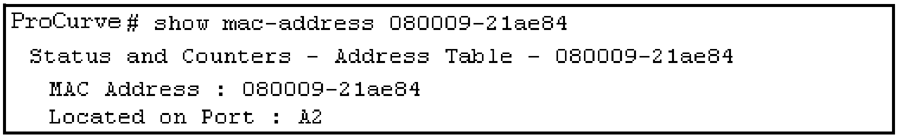
To List All Learned MAC Addresses on a VLAN, with Their Port Numbers. This command lists the MAC addresses associated with the ports for a given VLAN. For example:

ProCurve> show mac-address vlan 100

Note

The switches covered in this guide operate with a multiple forwarding database architecture.

To Find the Port On Which the Switch Learned a Specific MAC Address. For example, to find the port on which the switch learns a MAC address of 080009-21ae84:



```
ProCurve# show mac-address 080009-21ae84
 Status and Counters - Address Table - 080009-21ae84
  MAC Address : 080009-21ae84
  Located on Port : A2
```

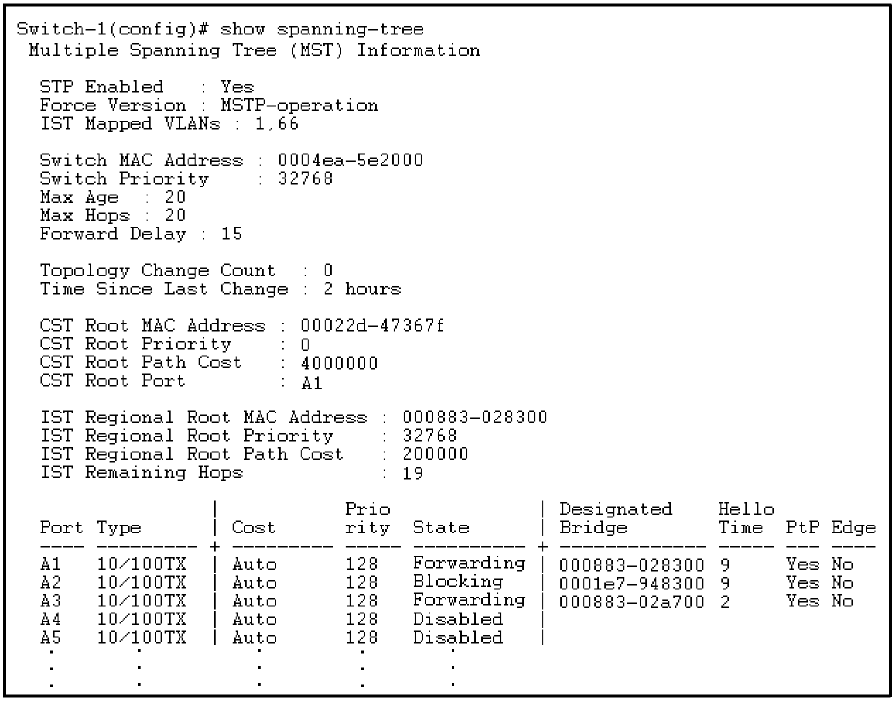
Spanning Tree Protocol (MSTP) Information

CLI Access to MSTP Data

This option lists the MSTP configuration, root data, and per-port data (cost, priority, state, and designated bridge).

Syntax: show spanning-tree

This command displays the switch's global and regional spanning-tree status, plus the per-port spanning-tree operation at the regional level. Note that values for the following parameters appear only for ports connected to active devices: **Designated Bridge**, **Hello Time**, **PtP**, *and* **Edge**.



```
Switch-1(config)# show spanning-tree
 Multiple Spanning Tree (MST) Information

  STP Enabled   : Yes
  Force Version : MSTP-operation
  IST Mapped VLANs : 1,66

  Switch MAC Address : 0004ea-5e2000
  Switch Priority    : 32768
  Max Age  : 20
  Max Hops : 20
  Forward Delay : 15

  Topology Change Count  : 0
  Time Since Last Change : 2 hours

  CST Root MAC Address : 00022d-47367f
  CST Root Priority    : 0
  CST Root Path Cost   : 4000000
  CST Root Port        : A1

  IST Regional Root MAC Address : 000883-028300
  IST Regional Root Priority    : 32768
  IST Regional Root Path Cost   : 200000
  IST Remaining Hops            : 19

                 |           Prio             | Designated    Hello
  Port Type      | Cost      rity  State      | Bridge        Time  PtP Edge
  ---- --------- + --------- ----- ---------- + ------------- ----- --- ----
  A1   10/100TX  | Auto      128   Forwarding | 000883-028300 9     Yes No
  A2   10/100TX  | Auto      128   Blocking   | 0001e7-948300 9     Yes No
  A3   10/100TX  | Auto      128   Forwarding | 000883-02a700 2     Yes No
  A4   10/100TX  | Auto      128   Disabled   |
  A5   10/100TX  | Auto      128   Disabled   |
   .       .         .        .       .
   .       .         .        .       .
   .       .         .        .       .
```

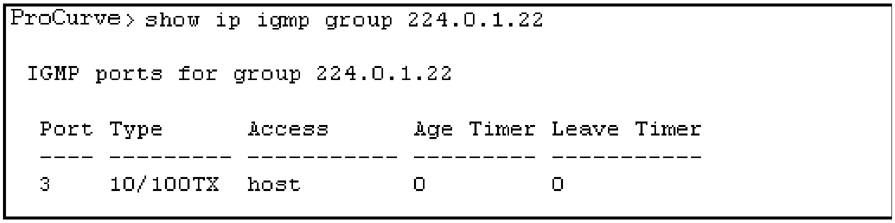
Figure B-14. Output from show spanning-tree Command

Internet Group Management Protocol (IGMP) Status

The switch uses the CLI to display the following IGMP status on a per-VLAN basis:

Show Command	Output
show ip igmp	Global command listing IGMP status for all VLANs configured in the switch: • VLAN ID (VID) and name • Active group addresses per VLAN • Number of report and query packets per group • Querier access port per VLAN
show ip igmp <*vlan-id*>	Per-VLAN command listing above IGMP status for specified VLAN (VID)
show ip igmp group <*ip-addr*>	Lists the ports currently participating in the specified group, with port type, Access type, Age Timer data and Leave Timer data.

For example, suppose that **show ip igmp** listed an IGMP group address of 224.0.1.22. You could get additional data on that group by executing the following:



```
ProCurve> show ip igmp group 224.0.1.22

 IGMP ports for group 224.0.1.22

  Port Type      Access      Age Timer Leave Timer
  ---- --------- ----------- --------- -----------
  3    10/100TX  host        0         0
```

Figure B-15. Example of IGMP Group Data

VLAN Information

The switch uses the CLI to display the following VLAN status:

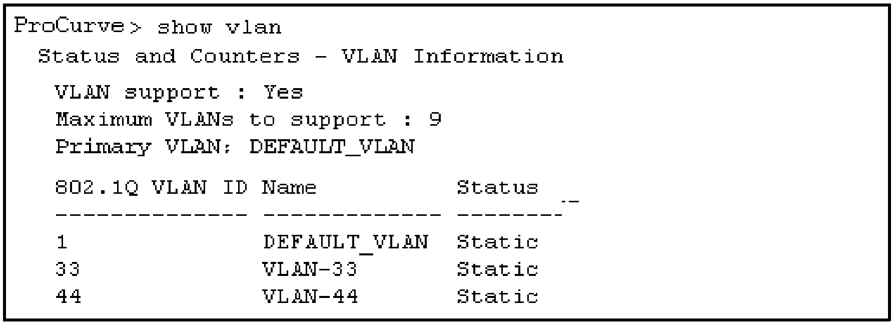
Show Command	Output
show vlan	Lists: • Maximum number of VLANs to support • Existing VLANs • Status (static or dynamic) • Primary VLAN
show vlan <*vlan-id*>	For the specified VLAN, lists: • Name, VID, and status (static/dynamic) • Per-Port mode (tagged, untagged, forbid, no/auto) • "Unknown VLAN" setting (Learn, Block, Disable) • Port status (up/down)

For example, suppose that your switch has the following VLANs:

PortsVLANVID
A1 - A12DEFAULT_VLAN 1
A1, A2VLAN-33 33
A3, A4VLAN-44 44

The next three figures show how you could list data on the above VLANs.

Listing the VLAN ID (VID) and Status for ALL VLANs in the Switch.

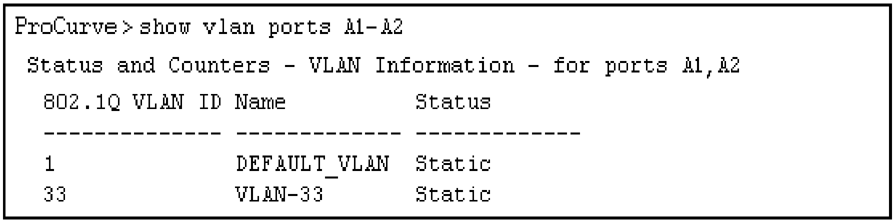


```
ProCurve> show vlan
 Status and Counters - VLAN Information

  VLAN support : Yes
  Maximum VLANs to support : 9
  Primary VLAN: DEFAULT_VLAN

  802.1Q VLAN ID Name          Status
  -------------- ------------- --------
  1              DEFAULT_VLAN  Static
  33             VLAN-33       Static
  44             VLAN-44       Static
```

Figure B-16. Example of VLAN Listing for the Entire Switch

Listing the VLAN ID (VID) and Status for Specific Ports.

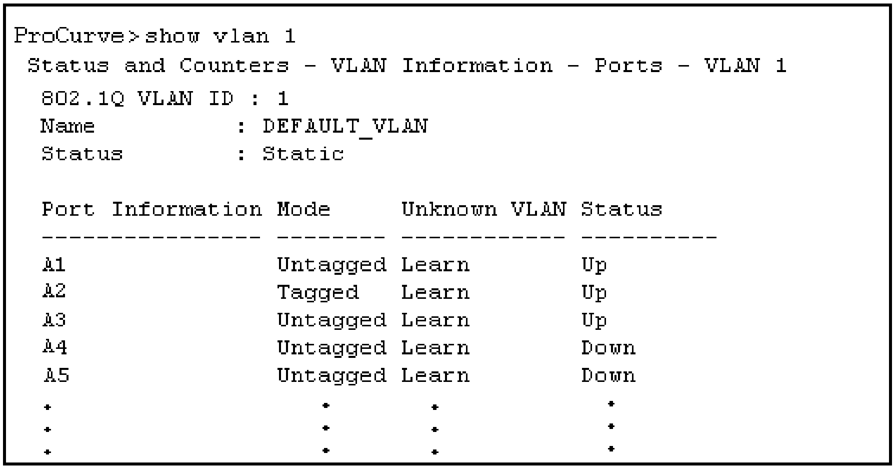
Because ports A1 and A2 are not members of VLAN-44, it does not appear in this listing.



```
ProCurve> show vlan ports A1-A2

 Status and Counters - VLAN Information - for ports A1,A2

  802.1Q VLAN ID Name          Status
  -------------- ------------- -------------
  1              DEFAULT_VLAN  Static
  33             VLAN-33       Static
```

Figure B-17. Example of VLAN Listing for Specific Ports

Listing Individual VLAN Status.



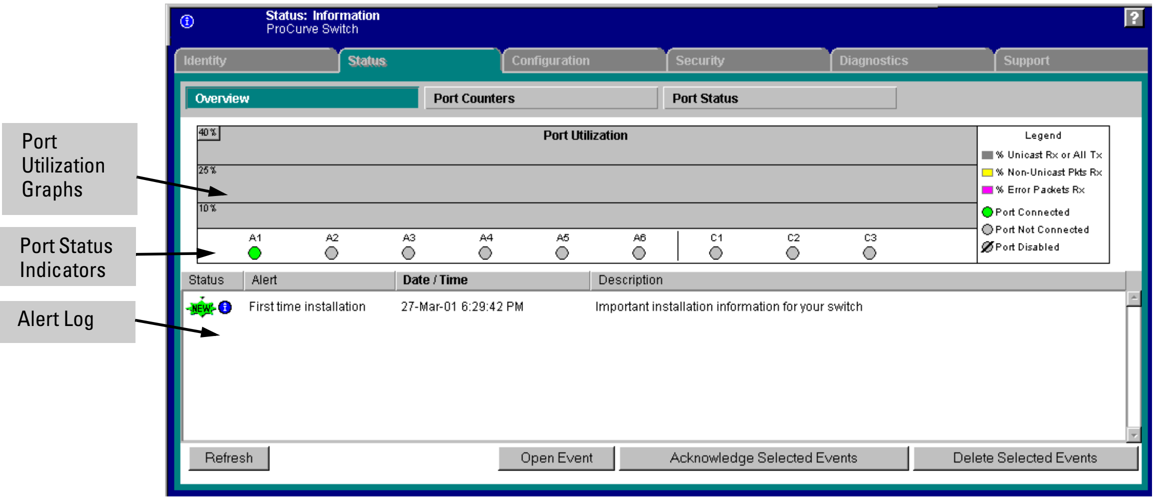
```
ProCurve> show vlan 1
 Status and Counters - VLAN Information - Ports - VLAN 1
  802.1Q VLAN ID : 1
  Name           : DEFAULT_VLAN
  Status         : Static

  Port Information Mode     Unknown VLAN Status
  ---------------- -------- ------------ ----------
  A1               Untagged Learn        Up
  A2               Tagged   Learn        Up
  A3               Untagged Learn        Up
  A4               Untagged Learn        Down
  A5               Untagged Learn        Down
  .                   .       .            .
  .                   .       .            .
  .                   .       .            .
```

Figure B-18. Example of Port Listing for an Individual VLAN

Web Browser Interface Status Information

The “home” screen for the web browser interface is the Status Overview screen, as shown below. As the title implies, it provides an overview of the status of the switch, including summary graphs indicating the network utilization on each of the switch ports, symbolic port status indicators, and the Alert Log, which informs you of any problems that may have occurred on the switch.

For more information on this screen, refer to the chapter titled “Using the ProCurve Web Browser Interface”.



Status	Alert	Date / Time	Description
NEW	First time installation	27-Mar-01 6:29:42 PM	Important installation information for your switch

Figure B-19. Example of a Web Browser Interface Status Overview Screen

Traffic Mirroring

Mirror Features

Feature	Default	Menu	CLI
Mirror CLI Quick Reference	n/a	n/a	B-40, B-41
Configure Mirror Source	disabled	page B-33	page B-44
Configure Mirror Destination at Source	disabled	page B-33	page B-46
Configure Remote Mirroring at Destination	disabled	n/a	page B-44
Display Mirror Configuration	n/a	page B-33	page B-61

Beginning with software release K.12.*xx*, traffic mirroring (Intelligent Mirroring) enables copying of network traffic from a network interface to a local or remote exit port where a host such as a traffic analyzer or intrusion detection system (IDS) is connected. This feature enables inspection of the traffic flowing on specific interfaces and can help in analyzing and debugging problems resulting from a misbehaving network or an individual client. This operation makes it easier to diagnose a network problem from a centralized location in a topology spread across a campus.

Note

Using the CLI, you can make full use of the switch's local and remote mirroring capabilities. Using the Menu interface, you can configure only local mirroring for either a single VLAN or a list composed of ports and/or static trunks.

Mirrored frames exceeding the allowed maximum transmission unit (MTU) size will be dropped. Also, the switch applies a 54-byte IPv4 header to mirrored frames. For more on these topics, including the jumbo and non-jumbo frame size limits, refer to "Maximum Supported Frame Size" on page B-73.

Intelligent Mirroring supports destinations on the local (source) switch and one or more remote switches, allowing traffic from a given mirroring session on a source switch to be sent to either a host on the same switch or bridged or routed to a host on another switch previously configured as the destination for that session.

- A switch can be configured as the destination for:
  - 32 remote mirroring sessions originating on other ProCurve switches running software release K.12.*xx*. This allows simultaneous mirroring sessions configured on multiple source switches to be directed to one or more exit ports on a given exit switch previously configured to support those sessions.

  - 4 local mirroring sessions originating on the same switch as the mirrored traffic

- A switch can be the originator (source) of four mirroring sessions, with each session mirroring traffic associated with a list composed of ports and/or static trunks, a mesh, or a VLAN interface.
- Options for mirroring criteria include:
  - Direction-Based mirroring for selecting traffic that is either entering or leaving the switch. In cases where you want to monitor traffic in only one direction, this improves utilization by reducing the amount of traffic sent to the monitoring destination.
  - Mirroring of all traffic entering or leaving the switch on the selected interface(s).
  - ACL (Access Control List) criteria to enable selective mirroring of individual IP traffic types entering the switch, including IP and specific source and/or destination criteria. This enables you to limit a given mirroring session to specific inbound traffic on a given interface (instead of all inbound traffic on the interface).
  - Source and/or destination MAC address used as mirroring criteria to select packets in inbound and/or outbound traffic on specified interfaces.

Terminology

Destination : For a given, local mirroring session on a switch, this is the exit port configured on that switch. For a given, remote mirroring session, this is the remote switch supporting the exit port you want to use. The destination for a given remote mirroring session should always be configured before the source is configured. (Refer to “Mirrored Traffic Destinations” on page B-29.)

Directional-Based Mirroring: On a given interface, using the direction of traffic movement (entering or leaving the switch, or both) as criteria for selecting which traffic to mirror.

Entry Port: On a remote mirroring destination switch, the port through which mirrored traffic is received from remote sources. (Does not apply to local mirroring.)

Exit Port: On the exit switch, the port to which a traffic analyzer or IDS is connected to receive mirrored traffic. For local mirroring, an exit port can be any available port to which a traffic analyzer or IDS is connected. For remote mirroring, the entry port and the exit port on the destination switch for a given session must belong to the same VLAN.

Exit Switch: The switch providing the (destination) exit port for mirrored traffic. Depending on how mirroring is configured, this can be either the mirroring source switch or a remote exit switch. See also *Local Exit Port*, *Remote Exit Switch*, and *Remote Exit Port*.

Host: Used in this chapter to refer collectively to a traffic analyzer or intrusion detection system (IDS).

IDS: Intrusion Detection System.

Local Exit Port: A port configured on a mirroring source switch as the port through which traffic from a specific local mirroring session leaves the switch. A traffic analyzer or IDS should be connected to this port. Up to four local mirroring sessions can be assigned to either the same local exit port or up to four different exit ports. (The exit switch also supports 32 remote mirroring session assignments, regardless of how many exit ports are used.) For local mirroring, the exit port can be any port on the switch that is not configured as a mirroring source. See also *Local Exit Port*.

Local Mirroring: The mirroring exit port and the mirroring source interface are on the same switch.

Mirroring Source Switch: A switch configured to mirroring inbound and/or outbound traffic to a destination on the same (local) switch or to a destination on a remote switch. This is the switch on which mirrored traffic originates.

Remote Exit Port: A port configured on a remote exit switch as the port through which traffic from a specific remote mirroring session leaves the switch. A traffic analyzer or IDS should be connected to this port. Up to 32 mirroring sessions can be assigned to the same remote exit port. (The exit switch supports a total of 32 remote mirroring session assignments, regardless of how many exit ports are used.) The mirrored traffic entry port for a given session and the exit port for that session must belong to the same VLAN. See also *Remote Exit Switch* and *Exit Switch*.

Caution

A mirroring exit port should be connected only to a network analyzer, IDS, or other network edge device that has no connection to other network resources. Allowing a mirroring exit port connection to a network can result in serious network performance problems, and is strongly discouraged by ProCurve Networking.

Remote Exit Switch: The destination switch for mirrored traffic when the source and destination of mirrored traffic are on different switches. Also termed the *Remote Destination Switch*.

Remote Mirroring: The mirroring exit port and the mirroring source interface are on different switches. In this case, IPv4 encapsulation is used to send the mirrored traffic from the source switch to the destination switch.

Source Switch: See *Mirroring Source Switch.*

Mirrored Traffic Destinations

Local Destinations

A local mirrored traffic destination is a port on the same switch as the source of the traffic being mirrored.

Remote Destinations

A *remote* mirrored traffic destination is a ProCurve switch configured to operate as the exit switch for mirrored traffic sessions originating on other ProCurve switches. As of June, 2007, switches capable of this operation include the following ProCurve switches:

- 3500yl
- 5400zl
- 6200yl
- 8212zl

Caution

Configuring a mirroring source switch with the destination and traffic selection criteria for a given mirroring session causes the switch to immediately begin mirroring traffic to that destination. In the case of remote mirroring, which uses IPv4 encapsulation, if the intended exit switch is not already configured as the destination for that session, its performance may be adversely affected by the stream of mirrored traffic. For this reason, ProCurve strongly recommends that you configure the exit switch for a remote mirroring session before configuring the source switch for that same session.

Mirrored Traffic Sources

You can designate mirroring for traffic entering or leaving the switch on:

- **ports and static trunks:** Provides the flexibility for mirroring on individual ports, groups of ports, and/or static port trunks.
- **meshed ports:** Enables traffic mirroring on all ports configured for meshing on the switch.
- **static VLANs:** Supports traffic mirroring on static VLANs configured on the switch. This option enables easy mirroring of traffic from all ports on a VLAN. It automatically adjusts mirroring to include traffic from newly added ports, and to exclude traffic from ports removed from the VLAN.

- **MAC addresses:** Enables mirroring on traffic selected according to a specified source and/or destination MAC address in packet headers.

Criteria for Selecting Traffic To Mirror

On the traffic sources listed above, you can use the following criteria to select traffic to mirror:

- direction of traffic movement (entering or leaving the switch, or both)
- type of IP traffic entering the switch, as defined by an ACL (Access Control List)
- source, destination, or both source and destination MAC addresses in packet headers

Mirrored Traffic Operation and Options

Switches running software release K.12.xx or greater support the following:

- four mirroring destinations configured to correspond to local mirroring source sessions
- 32 mirroring destinations configured to correspond to remote mirroring source sessions
- four local or remote mirroring source sessions

Mirroring Sessions

A mirroring source can be a port or static-trunk list, mesh, VLAN, or MAC address. A mirroring source and a mirroring destination comprise a given mirroring session. For any session, the destination must be a single (exit) port. (It cannot be a trunk, VLAN, or mesh.) Multiple mirroring sessions can be mapped to the same exit port, which provides flexibility in distributing hosts such as traffic analyzers or an IDS. On the mirroring destination switch, the port through which the mirrored traffic for a given session enters the switch and the exit port for that same session must belong to the same VLAN. (Refer to "2. Configure the Remote Mirroring Session on Destination Switch" on page B-44.)

Each of the four mirroring sessions supported at a mirroring source can have either the same or a different destination. Destination options include an exit port on the source (local) switch and/or on one remote ProCurve switch configured to support remote mirroring. This offers the following benefits:

- Mirrored traffic belonging to each session can be directed to the same destination or to different destinations.

- You can reduce the risk of oversubscribing a single exit port by directing traffic from different session sources to different exit ports
- You can segregate traffic by type, direction, or source.

A given switch can operate as both a source and a destination for mirroring sessions.

Configuration

Table B-1 lists the traffic mirroring configuration support available through the CLI, Menu Interface, and SNMP methods.

Table B-1. Traffic Mirroring Configuration Options

Configuration Level	Monitor	Traffic Direction		
		CLI Config	Menu and Web I/F Config[1]	SNMP Config
VLAN	all traffic	inbound only, outbound only, or both directions	inbound and outbound combined	inbound only, outbound only, or both directions
	ACL-selected (IP) traffic	Inbound only	n/a	n/a

Port(s)
Trunk(s)
Mesh
	all traffic	inbound only, outbound only, or both directions	inbound and outbound combined	inbound only, outbound only, or both directions

	ACL-selected (IP) traffic	Inbound only	n/a	n/a
Switch (global)	MAC-based traffic selection	inbound only, outbound only, or both directions	n/a	inbound only, outbound only, or both directions

[1] Configures only session 1, and only for local mirroring.

Note

Using the CLI, you can access all mirroring capabilities on the switch. Using the Menu or Web interfaces, you can configure and display only session 1 and only as a local mirroring session for traffic in both directions on the specified interface. If session 1 has been configured in the CLI for local mirroring for inbound-only or outbound-only traffic, then using the Menu or Web interface to change the session 1 configuration *automatically* reconfigures the session to monitor both inbound and outbound traffic on the interface. (If session 1 has been configured in the CLI with an ACL or as a remote mirroring session, then the Menu and Web interfaces cannot be used to configure a mirroring session.) The CLI can configure sessions 1 - 4 for local or remote mirroring in any combination, and can be used to override a Menu or Web interface configuration of session 1. Using SNMP allows the same capability and effect as the CLI *except* that SNMP cannot be used to configure any ACL mirroring. (SNMP can overwrite an existing configuration for any session.)

Endpoint Switches and Intermediate Devices

The endpoint switches used for remote mirroring source and remote mirroring exit functions must be ProCurve switches that support the mirroring functions described in this chapter. However, because remote mirroring on your ProCurve switch uses IPv4 encapsulation of mirrored traffic to remote destination switches, the intermediate switches and routers in a layer 2/3 domain can be from any vendor supporting IPv4.

Notes

The exit interface for a mirroring destination must be an individual port.

The switch mirrors traffic on static trunks, but not on dynamic LACP trunks.

The switch mirrors traffic at line rate. When mirroring multiple interfaces in networks with high traffic levels, it is possible to copy more traffic to a mirroring destination than the link supports. In this case, some mirrored traffic may not reach the destination. If you are mirroring a high traffic volume, distribute the load to multiple exit ports if possible.

Updating from a Legacy Mirroring Configuration

On a switch running a software version earlier than K.12.*xx* and also configured for mirroring, downloading and booting from software release K.12.*xx* or greater produces the following mirroring configuration:

- The legacy port or VLAN mirroring configuration maps to session 1.
- Selection criteria for session 1 is set to **both** (that is, mirroring traffic entering and leaving the switch on the configured interface).
- The local exit port in the legacy configuration is applied to session 1.

Notes

Booting from Software Versions Earlier than K.12.*xx*: If it is necessary to boot the switch from a legacy (pre-K.12.xx) software version after using version K.12.*xx* or greater to configure mirroring, remove mirroring from the configuration before booting with the earlier software.

Maximum Supported Frame Size: The IPv4 encapsulation of mirrored traffic adds a 54-byte header to each mirrored frame. If a resulting frame exceeds the MTU (Maximum Transmission Unit) allowed in the path from the mirroring source to the mirroring destination, the frame is dropped. For more information, refer to "Maximum Supported Frame Size" on page B-73.

No Frame Truncation: Mirroring does not truncate frames, and oversized mirroring frames will be dropped. Also, remote mirroring does not allow downstream devices in a mirroring path to fragment mirrored frames.

Using the Menu or Web Interface To Configure Local Mirroring

Menu and Web Interface Limits

The Menu and Web interfaces can be used to quickly configure or reconfigure local mirroring on session 1, and allow one of the following two mirroring source options:

- any combination of source port(s), trunk(s), and/or a mesh
- one static, source VLAN interface

The Menu and Web interfaces also have these limits:

- Configure and display only session 1 and only as a local mirroring session for traffic in *both* directions on the specified interface. (Selecting inbound-only or outbound-only is not an option.)
- If session 1 has been configured in the CLI for local mirroring for inbound-only or outbound-only traffic on one or more interfaces, then using the Menu or Web interface to change the session 1 configuration *automatically reconfigures the session* to monitor both inbound and outbound traffic on the designated interface(s).
- If session 1 has been configured in the CLI with an ACL or as a remote mirroring session, then the Menu and Web interfaces are not available for changing the session 1 configuration.
- The CLI (and SNMP) can be used to override any Menu or Web interface configuration of session 1.

Configuration Steps

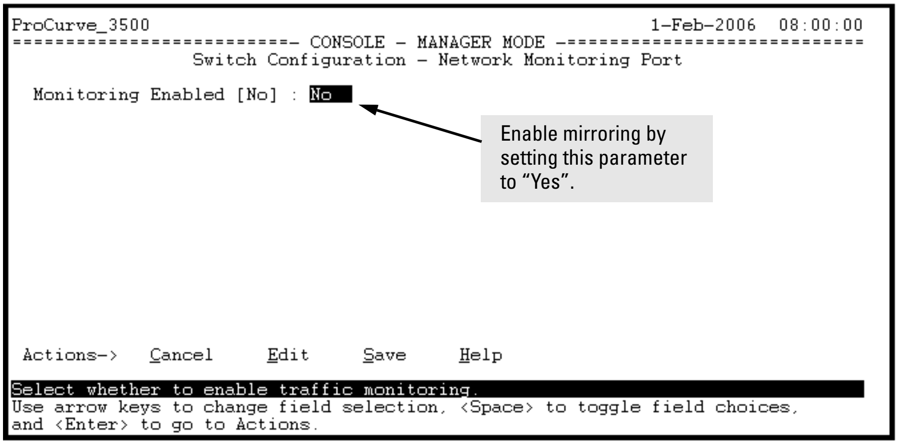
Notes

If mirroring has already been enabled on the switch, the Menu screens will appear differently than shown in this section.

1. From the Main Menu, Select:

   2. Switch Configuration...

   3. Network Monitoring Port

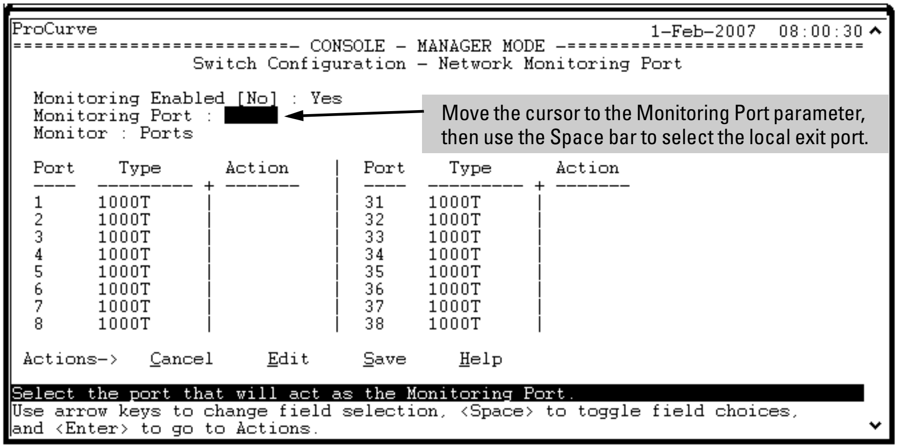


```
ProCurve_3500                                            1-Feb-2006  08:00:00
==========================- CONSOLE - MANAGER MODE -===========================
                 Switch Configuration - Network Monitoring Port

  Monitoring Enabled [No] : No

 Actions->   Cancel     Edit     Save     Help

Select whether to enable traffic monitoring.
Use arrow keys to change field selection, <Space> to toggle field choices,
and <Enter> to go to Actions.
```

Enable mirroring by setting this parameter to "Yes".

Figure B-20. The Default Network Mirroring Configuration Screen

2. In the Actions menu, press **[E]** (for `Edit`).
3. If mirroring is currently disabled for session 1 (the default), then enable it by pressing the Space bar (or **[Y]**) to select `Yes`.
4. Press the down arrow key to display a screen similar to the following and move the cursor to the **Monitoring Port** parameter.



```
ProCurve                                                         1-Feb-2007   08:00:30
=========================- CONSOLE - MANAGER MODE -===========================
                 Switch Configuration - Network Monitoring Port

  Monitoring Enabled [No] : Yes
  Monitoring Port :
  Monitor : Ports

  Port    Type       Action       |  Port    Type       Action
  ----   --------- + -------      |  ----   --------- + -------
  1      1000T     |              |  31     1000T     |
  2      1000T     |              |  32     1000T     |
  3      1000T     |              |  33     1000T     |
  4      1000T     |              |  34     1000T     |
  5      1000T     |              |  35     1000T     |
  6      1000T     |              |  36     1000T     |
  7      1000T     |              |  37     1000T     |
  8      1000T     |              |  38     1000T     |

 Actions->    Cancel     Edit      Save      Help

Select the port that will act as the Monitoring Port.
Use arrow keys to change field selection, <Space> to toggle field choices,
and <Enter> to go to Actions.
```

Move the cursor to the Monitoring Port parameter, then use the Space bar to select the local exit port.

Figure B-21. How To Select a Local Exit Port

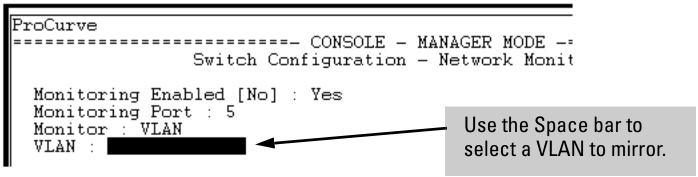
5. Use the Space bar to select the port to use for sending mirrored traffic to a locally connected traffic analyzer or IDS. (The selected interface must be a single port. It cannot be a trunk or mesh.) In this example, port 5 is selected as the local exit port.

6. Highlight the Monitor field and use the Space bar to select the interfaces to mirror:

   Ports: Use for mirroring ports, static trunks, or the mesh.

   VLAN: Use for mirroring a VLAN.

7. Do one of the following:
   - If you are mirroring ports, static trunks, or the mesh, go to step 8.
   - If you are mirroring a VLAN:
     i. Press **[Tab]** or the down arrow key to move to the **VLAN** field.

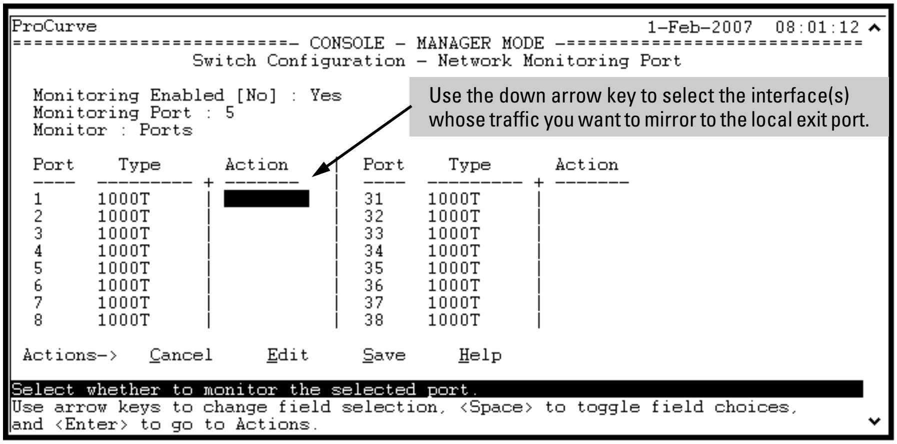


```
ProCurve
=========================- CONSOLE - MANAGER MODE -=
                  Switch Configuration - Network Monit

  Monitoring Enabled [No] : Yes
  Monitoring Port : 5
  Monitor : VLAN
  VLAN :
```

Use the Space bar to select a VLAN to mirror.

     ii. Use the Space bar to select the VLAN you want to mirror.
     iii. Go to step 10.

8. Use the down arrow key to move the cursor to the **Action** column for the individual port interfaces and position the cursor at a port, trunk, or mesh you want to mirror.



```
ProCurve                                                   1-Feb-2007  08:01:12
=========================- CONSOLE - MANAGER MODE -===========================
                 Switch Configuration - Network Monitoring Port

  Monitoring Enabled [No] : Yes
  Monitoring Port : 5
  Monitor : Ports

  Port   Type        Action      |  Port   Type        Action
  ----   ---------- + -------    |  ----   ---------- + -------
  1      1000T      |            |  31     1000T      |
  2      1000T      |            |  32     1000T      |
  3      1000T      |            |  33     1000T      |
  4      1000T      |            |  34     1000T      |
  5      1000T      |            |  35     1000T      |
  6      1000T      |            |  36     1000T      |
  7      1000T      |            |  37     1000T      |
  8      1000T      |            |  38     1000T      |

 Actions->   Cancel     Edit     Save     Help

Select whether to monitor the selected port.
Use arrow keys to change field selection, <Space> to toggle field choices,
and <Enter> to go to Actions.
```

Use the down arrow key to select the interface(s) whose traffic you want to mirror to the local exit port.

9. Press the Space bar to select **Monitor** for the port(s) and/or trunk(s) and/or mesh that you want mirrored. Use the down arrow key to move from one interface to the next in the **Action** column. (If the mesh or any trunks are configured, they will appear at the end of the port listing.)

10. When you finish selecting interfaces to mirror, press **[Enter]**, then press **[S]** (for **Save**) to save your changes and exit from the screen.

11. Return to the Main Menu.

CLI: Configuring Local and Remote Mirroring

Command	Page
Quick Reference	
Local Mirroring Commands	B-40
Remote Mirroring Commands	B-41
Configuring a Session Destination on a Remote Exit Switch	
mirror endpoint ip	
< *src-ip* > < *src-udp-port* > < *dst-ip* > < *port-#* >	B-44
Configuring a Local Destination on a Session Source Switch	B-46
mirror < 1 - 4 > [name < *name-str* >] port < *port-#* >	
Configuring a Remote Destination on a Session Source Switch	
mirror < 1 - 4 > [name < *name-str* >] remote ip	
< *src-ip* > < *src-udp-port* > < *dst-ip* >	B-47
Defining Traffic To Mirror on a Session Source Switch	
interface < *port*/*trunk*/mesh > monitor	
all < in | out | both > mirror	B-50
ip access-group < *acl-name* > in mirror	B-54
vlan < *vid-#* > monitor	
all < in | out | both > mirror	B-52
ip access-group < *acl-name* > in mirror	B-56
monitor mac < *mac-addr* > < src | dest | both > mirror	B-57
Display Commands	B-61
show monitor [endpoint | 1 - 4 | name < *name-str* >]	
Mirroring Examples	B-68
Maximum Frame Size	B-73
Operating Notes	B-75

Using the CLI you can configure a mirroring session to an exit port on either the same switch as the source interface (local mirroring) or on another switch (remote mirroring). (The remote switch must be a ProCurve switch offering the full mirroring capabilities described in this chapter.)

General Steps for Using the CLI To Configure Mirroring

Caution

Configuring a switch with the destination and traffic selection criteria for a given mirroring session causes the switch to immediately begin mirroring traffic to that destination. In the case of remote mirroring, which uses IPv4 encapsulation, if the intended exit switch is not already configured as the destination for that session, its performance may be adversely affected by the stream of mirrored traffic. For this reason, ProCurve strongly recommends that you configure the exit switch for a remote mirroring session before configuring the source switch for that same session.

Remote Mirroring (Mirroring Source and Destination on Different Switches).

1. Determine the session IP addressing, UDP port number, and destination (exit) port number for the remote session:
   - source VLAN or subnet IP address on the source switch
   - destination VLAN or subnet IP address on the destination switch
   - random UDP port number for the session (7933-65535)
   - exit port on destination switch (Must belong to the same VLAN as the port through which the remotely mirrored traffic for the session enters the switch.)

   (For a given session, the IP addressing and UDP port number selected in this step must be used on both the source and destination switches.)

2. On the mirroring *destination* (exit) switch, use the **mirror endpoint** command with the information from step 1 to configure a mirroring session to a specific exit port.

3. Determine the session identity (1 - 4) and (optional) alphanumeric name to use on the mirroring *source* switch.

4. Determine the traffic to be filtered by any of the following selection methods and the appropriate configuration level (VLAN, port, mesh, trunk, global):
   - Direction: inbound, outbound, or both
   - inbound ACL (IP addresses)
   - MAC addresses: source and/or destination

5. On the mirroring *source* switch:

   a. Use the **mirror** command with the selected session identity (1 - 4) and the IP addresses and UDP port number from step 1, to configure a mirroring session.

b. Use one of the following commands to configure the mirroring source(s) selected in step 4 and assign them to the configured session:
interface < *port/trunk/mesh* **> monitor**
vlan < *vid* **> monitor**
monitor mac < *mac-addr* **>**

After you complete step 5b, the switch begins mirroring traffic to the remote destination for the configured session.

Local Mirroring (Mirroring Source and Destination on the Same Switch).

1. Determine the session identity and local destination port:
   - session number (1-4) and (optional) alphanumeric name
   - exit port (This can be any port on the switch except a mirroring source port.)
2. Use **mirror < 1 - 4 > [name < name-str >] port < port-# >** to configure the session.
3. Determine the traffic to be filtered by any of the following selection methods and the appropriate configuration level (VLAN, port, mesh, trunk, switch):
   - – Direction: inbound, outbound, or both
   - – inbound ACL (IP addresses)
   - – MAC addresses: source and/or destination
4. Use the **monitor** command to assign the source interface(s) to the session.

After completing step 4, the switch begins mirroring traffic to the configured exit port.

The next two sections provide quick references to the command syntax options for executing the above general steps.

Quick Reference to Local Mirroring Set-Up

These commands configure or remove mirroring where the mirroring source and destination are on the same switch. For command syntax details, refer to the pages listed after each heading. For each mirroring Source Switch option:

- The **mirror** command identifies the destination for the mirroring session.
- The **interface** and **vlan** commands identify the mirroring source; that is, the interface type, the traffic to mirror, and the mirroring session to use.

To Configure or Remove a Local Mirroring Session
Mirroring Session Number, Exit Port, and (Optional) Session Name (Page B-46)

```
mirror < 1 - 4 > port < port-# > [ name < name-str >]
no mirror < 1 - 4 >
```

The **no** form of the command removes the mirroring session and any mirroring source previously assigned to that session by the following commands.

To Configure or Remove Mirroring on Port/Trunk/Mesh Interfaces for Local Sessions:

Directional Criteria Selects Traffic To Mirror (Page B-50).

```
[no] interface < port/trunk/mesh > monitor all < in | out | both > mirror
        < 1 - 4 | name-str > [< 1 - 4 | name-str > < 1 - 4 | name-str > < 1 - 4 | name-str >]
```

Inbound ACL Criteria Selects Traffic To Mirror (Page B-54).

```
[no] interface < port/trunk/mesh > monitor ip access-group < acl-name > in mirror
        < 1 - 4 | name-str > [< 1 - 4 | name-str > < 1 - 4 | name-str > < 1 - 4 | name-str >]
```

The **< name-str >** option applies only if the specified mirroring session has already been configured with the **name < name-str >** option in the **mirror** command.

The **no** form of the command removes the ***< port/trunk/mesh >*** mirroring source from the specified session, but leaves the session available for other assignments.

To Configure or Remove Mirroring on VLAN Interfaces for Local Sessions:

Directional Criteria Selects Traffic To Mirror (Page B-52)

```
[no] vlan < vid-# > monitor all < in | out | both > mirror < 1 - 4 | name-str >
        [< 1 - 4 | name-str > < 1 - 4 | name-str > < 1 - 4 | name-str >]
```

Inbound ACL Criteria Selects Traffic To Mirror (Page B-56).

```
[no] vlan < vid-# > monitor ip access-group < acl-name > in mirror < 1 - 4 | name-str >
        [< 1 - 4 | name-str > < 1 - 4 | name-str > < 1 - 4 | name-str >]
```

The **< name-str >** option applies only if the mirroring session has already been configured with the **name < name-str >** option in the **mirror** command.

The **no** form of the command removes **vlan <** ***vid-#*>** mirroring source from the specified session, but leaves the session available for other assignments.

Note

If session 1 is already configured with a destination, you can execute **[no] vlan < vid > monitor** or **[no] interface < port > monitor** without mirroring criteria and a mirror session number. In this case, the switch automatically configures or removes mirroring for inbound and outbound traffic from the specified VLAN or port(s) to the destination configured for session 1.

To Configure or Remove MAC-based Mirroring on a Source Switch for Local Sessions (Page B-57):

```
[no] monitor mac < mac-addr > < src | dest | both >  mirror < 1 - 4 | name-str >
        [< 1 - 4 | name-str > < 1 - 4 | name-str > < 1 - 4 | name-str >]
```

Enter the **monitor mac mirror** command at the global configuration level.

Use the **no** form of the complete command syntax (for example, **no monitor mac 112233-445566 src mirror 3**) to remove a MAC address as mirroring criteria from an active session on the switch without removing the session itself.

Quick Reference to Remote Mirroring Set-Up

These commands configure mirroring where the mirrored traffic source and destination are on different switches. For each mirroring source switch option:

- The **mirror** command identifies the destination for the mirroring session.
- The **interface** and **vlan** commands identify the interface type, the traffic to mirror, and the mirroring session to use for the selected traffic

For command syntax details, refer to the pages listed after each heading.

Caution

When configuring a remote mirroring session, always configure the destination switch first. Configuring the source switch first can result in a large volume of mirrored, IPv4-encapsulated traffic arriving at the destination without an exit path, which can slow switch performance.

To Enable or Disable a Remote Mirroring Destination on the Switch:

This command is executed on a destination switch and designates the exit port to use with a mirroring session you will configure on another switch used as a mirroring source. The data used for this match on the destination switch includes:

- the unique UDP port number you plan use in the mirroring session configuration in the source switch (recommended range: 7933-65535)

- the source and destination IP addresses you plan to use in the mirroring session configuration in the source switch
- the port number of the exit port you want to use on the destination switch

Source Data Relates Mirrored Session to Exit Port on Destination Switch (Page B-44):

```
mirror endpoint ip < src-ip-addr > < src-udp-port > < dst-ip-addr > port < port-# >
no mirror endpoint ip < src-ip-addr > < src-udp-port > < dst-ip-addr >
```

(On the destination switch, the mirrored traffic entry port for a given session and the exit port for that session must belong to the same VLAN.)

To Configure or Remove a Mirroring Session on a Source Switch

Defines a Remote Mirroring Session on a Source Switch (Page B-46):

```
mirror < 1 - 4 > [name < name-str >] remote ip < src-ip > < src-udp-port > < dst-ip >
no mirror < 1 - 4 >
```

The **no** command form removes both the mirroring session and any mirroring source(s) previously assigned to the session by the following commands.

To Configure Port or Trunk Mirroring on a Source Switch:

Directional Criteria Selects Traffic To Mirror (Page B-50):

```
[no] interface < port/trunk/mesh > monitor all < in | out | both > mirror
       < 1 - 4 | name-str > [< 1 - 4 | name-str > < 1 - 4 | name-str > < 1 - 4 | name-str >]
```

Inbound ACL Criteria Selects Traffic To Mirror (Page B-54):

```
[no] interface < port/trunk/mesh  > monitor ip access-group < acl-name > in mirror
       < 1 - 4 | name-str > [< 1 - 4 | name-str > < 1 - 4 | name-str > < 1 - 4 | name-str >]
```

The **< name-str >** option applies only if the specified mirroring session has already been configured with the **name < name-str >** option in the **mirror** command.

The **no** command form removes the ***< port/trunk/mesh >*** mirroring source from the specified session, but leaves the session available for other assignments.

To Configure VLAN Mirroring on a Source Switch:

Directional Criteria Selects Traffic To Mirror (Page B-52):

```
[no] vlan < vid-# >  monitor all < in | out | both > mirror < 1 - 4  | name-str >
        [< 1 - 4  | name-str > < 1 - 4  | name-str > < 1 - 4  | name-str >]
```

Inbound ACL Criteria Selects Traffic To Mirror (Page B-56:

```
[no] vlan < vid-# > monitor ip access-group < acl-name > in mirror < 1 - 4 | name-str >
        [< 1 - 4  | name-str > < 1 - 4  | name-str > < 1 - 4  | name-str >]
```

The **< name-str >** option applies only if the specified mirroring session has already been configured with the **name < name-str >** option in the **mirror** command.

The **no** command form removes **vlan <** ***vid-#*** **>** mirroring source from the specified session, but leaves the session available for other assignments.

Note

If session 1 is already configured with a destination, you can execute **[no] vlan < vid > monitor** or **[no] interface < port > monitor** without mirroring criteria and a mirror session number. In this case, the switch automatically configures or removes mirroring for inbound and outbound traffic from the specified VLAN or port(s) to the destination configured for session 1.

To Configure or Remove MAC-based Mirroring on a Source Switch for Remote Sessions (Page B-57):

```
[no] monitor mac < mac-addr > < src | dest | both >  mirror < 1 - 4 | name-str >
        [< 1 - 4 | name-str > < 1 - 4 | name-str > < 1 - 4 | name-str >]
```

Enter the **monitor mac mirror** command at the global configuration level.

Use the **no** form of the complete command syntax (for example, **no monitor mac 112233-445566 src mirror 3**) to remove a MAC address as mirroring criteria from an active session on the switch without removing the session itself.

1. Determine the Mirroring Session Identity and Destination

For a Local Mirroring Session. Determine the port number for the exit port (such as A5, B10, etc.), then go to "4. Configure Mirroring Sources" on page B-49.

For a Remote Mirroring Session. Determine the following and then go to step 2, below.

- the IP address of the VLAN or subnet on which the exit port exists on the destination switch
- the port number for the desired exit port on the destination switch (On the destination switch, the mirrored traffic entry port for a given remote mirroring session and the exit port for that session must belong to the same VLAN.)
- the IP address of the VLAN or subnet on which the mirrored traffic enters or leaves the source switch
- the unique UDP port number to use for the session (The recommended range is 7933-65535. Refer to the following "Caution".)

Caution

Although the switch allows use of UDP port numbers in the range of 1 to 65535, UDP port numbers below 7933 are reserved for various IP applications. Using them for mirroring can result in disrupting other IP functions, and can also result in non-mirrored traffic received on the destination switch being sent to a mirroring exit port.)

2. Configure the Remote Mirroring Session on Destination Switch

This step is needed when the exit port for a mirroring session is on a different switch than the mirroring source. (For local mirroring, go to step 3 on page B-49.) In this case, the mirroring destination switch must be configured to recognize each unique mirroring session and assign its traffic to an exit port before the source switch is configured to send mirrored traffic. This is done by configuring the destination switch with the values determined for remote mirroring in step 1, above.

Note

A switch operating as a destination for mirrored traffic sessions can support 32 different remote sessions (and 4 local sessions). Multiple sessions can be assigned to the same exit port or distributed to multiple exit ports.

Syntax: mirror endpoint ip < *src-ip* > < *src-udp-port* > < *dst-ip* > < *port-#* >
no mirror endpoint ip < *src-ip* > < *src-udp-port* > < *dst-ip* >

This command is used on a destination switch to establish the endpoint for a specific mirroring session you will configure on a remote mirroring source switch. The command uniquely associates the mirrored traffic from the desired session on the source switch with a specific exit port on the destination switch. This is done by using the same set of source and destination identifiers when configuring the same session on both the source and destination switches. Thus, for a given mirroring session, the **<src-ip >**, **< src-udp-port >** *and* **< dst-ip >** *for the* **mirror endpoint** *command must be the same on both switches. To see this correspondence, refer to the* **mirror** *command syntax under "Configuring a Source Switch for a Mirroring Destination on a Remote Switch" on page B-47.*

The **no** *form of the command deletes the mirroring endpoint support for the configured session on the remote destination switch.*

Caution: *Mirroring endpoint support for a given session should not be removed if there are any remote source switches currently configured to mirroring traffic to the endpoint for that session. See also the Caution on page B-41.*

< src-ip > : *Must exactly match the* **< src-ip >** *setting you will configure in the source switch for the remote mirroring session the exit switch is being configured to support.*

< src-udp-port > : *Must exactly match the* **< src-udp-port >** *setting you will configure in the source switch for the remote mirroring session the exit switch is being configured to support. (The recommended range is 7933-65535.)*

This setting associates the source mirroring session with the desired **mirror endpoint**.*by using the same, unique UDP port number to identify a given mirroring session on a source switch and the session's corresponding destination on a remote exit switch.*

< dst-ip >: *Must exactly match the* **< dst-ip >** *setting configured in the source switch for the remote mirroring session the exit switch is being configured to support.*

Syntax: mirror endpoint ip < *src-ip* > < *src-udp-port* > < *dst-ip* > < *port-#* >
no mirror endpoint ip < *src-ip* > < *src-udp-port* > < *dst-ip* >

> **< port-# >:** *Exit port for mirrored traffic from the specified session. This is the port to which a traffic analyzer or IDS should be connected.*

3. Configure the Mirroring Session on the Source Switch

For local mirroring, only a session number and a destination port number are needed. (You also have the option of associating a name with the session number.) Refer to "Configuring Mirroring with a Destination on the Local (Source) Switch" below.

If the mirroring destination is on a remote switch instead of the local (source) switch, then the traffic source IP address, the mirroring destination IP address, and a unique (randomly selected) UDP port number are required for the mirroring session. (Refer to page B-47.)

Configuring Mirroring with a Destination on the Local (Source) Switch. For a given mirroring session on a source switch, use this command to specify the exit port to use on the same switch. To create the mirroring session itself, refer to the options under "1. Determine the Mirroring Session Identity and Destination" on page B-44.

Syntax: mirror < 1 - 4 > port < *port-#* > [name < *name-str* >]
no mirror < 1- 4 >

> *This command assigns the exit port to use for the specified mirroring session, and must be executed from the global configuration level.*
>
> *The* **no** *form of the command removes the mirroring session and any mirroring source previously assigned to that session. To preserve the session while deleting a mirroring source assigned to it, refer to the* **no** *command descriptions under "4. Configure Mirroring Sources" on page B-49.*
>
> **< 1 - 4 > :** *Identifies the mirroring session created by this command. (Multiple sessions on the switch can use the same exit port.)*
>
> **name < name-str > :** *Optional alphanumeric name string used to identify the session. Can be up to 15 characters in length.*

Syntax: mirror < 1 - 4 > port < *port-#* > [name < *name-str* >]
no mirror < 1- 4 >

> **port < port-# > :** *Exit port for mirrored traffic from the specified session. This is the port to which a traffic analyzer or IDS should be connected.*

Configuring a Source Switch for a Mirroring Destination on a Remote Switch. Use this command when you want to mirroring traffic from a source switch to an exit port on a remote mirroring destination switch. For a given session, the values for the fields in this command should already be configured in the destination switch. (Refer to steps 1 and 2 on page B-44.)

Caution

Configuring a switch with the traffic selection criteria and destination for a given mirroring session starts traffic mirroring to that destination. In the case of remote mirroring, which uses IPv4 encapsulation, if the intended exit switch is not already configured as the destination for that session, its performance may be adversely affected by the stream of mirrored traffic. For this reason, ProCurve strongly recommends that you configure the exit switch for a remote mirroring session, as described under “2. Configure the Remote Mirroring Session on Destination Switch” on page B-44, before using the command in this section to configure the source switch for that same session.

Syntax: [no] mirror < 1 - 4 > [name < *name-str* >] remote ip < *src-ip* >
< *src-udp-port* > < *dst-ip* >

> *This command is used on the source switch to uniquely associate the mirrored traffic from a specific mirroring session with a specific, remote exit switch. Thus, for a given mirroring session, the same source and destination values should be configured on both the mirroring destination switch and the mirroring source switch.(Each remote mirroring session having the same source and destination IP addresses should have a unique UDP port value.)*
>
> *When you execute this command, this message appears:*
>
> **Caution: Please configure destination switch first.**
> **Do you want to continue [y/n]?**
>
> - *If you have not yet configured the session on the mirroring destination switch, use the instructions in step 2 on page B-44 to do so before using this command.*
> - *If you previously configured the session on the mirroring destination switch, type* **y** *(for “yes”) to complete this command.*

Syntax: [no] mirror < 1 - 4 > [name < *name-str* >] remote ip < *src-ip* > < *src-udp-port* > < *dst-ip* >

The **no** *form of the command removes the mirroring session and any mirroring source previously assigned to that session. To preserve the session while deleting a mirroring source assigned to it, refer to the* **no** *command descriptions under "4. Configure Mirroring Sources" on page B-49.*

< 1 - 4 > : *Identifies the mirroring session created by this command.*

name < name-str >: *Optional alphanumeric name string used as an additional session identifier. Can be up to 15 characters in length.*

< src-ip > : *The IP address of the VLAN or subnet on which the traffic to be mirrored enters or leaves the switch.*

< src-udp-port > : *This value associates the configured mirroring session with a UDP port number. Where multiple sessions have the same source IP address (***< src-ip >***) and destination IP address (***<** ***dst-ip*** **>***), the UDP port number should be unique for each session. The UDP port number used for a given session should be in the range of 7933 - 65535.*

> ***Caution:*** *UDP port numbers below 7933 are reserved for various IP applications. Using them for mirroring can result in disrupting other IP functions, and can also result in non-mirrored traffic received on the destination switch being sent to a mirroring exit port.)*

*The configured UDP port number is included in the frames mirrored from the source switch to the remote exit switch (***mirror endpoint***), and enables the exit switch to match the frames to the exit port configured for that combination of UDP port number, source IP address, and destination IP address. To see this correspondence, refer to the* **mirror endpoint** *command syntax under "2. Configure the Remote Mirroring Session on Destination Switch" on page B-44.*

< ***dst-ip*** **>:** *For the mirroring session specified in the command, this is the IP address of the VLAN or subnet on which the desired remote exit port exists. (The exit port is specified in the mirroring configuration on the exit switch, and a traffic analyzer or IDS should be connected to this port.) Refer to "2. Configure the Remote Mirroring Session on Destination Switch" on page B-44.*

4. Configure Mirroring Sources

This action configures a source switch with the criteria for selecting the traffic to mirror, and assigns the configured source criteria to a previously configured mirroring session.

Traffic Selection Options

To configure traffic mirroring, you must determine the interface, direction, and selection criteria for the traffic you want to mirror from the following options:

- interface type
  - port, trunk, and/or mesh
  - VLAN
  - switch (global configuration level)
- traffic direction and mirroring criteria
  - all traffic inbound, outbound, or both
  - ACL-filtered IP traffic type (inbound-only)
  - MAC address (source and/or destination)

Mirroring Source Limits

For a given mirroring session you can configure any *one* of the following mirroring source options:

- multiple ports, trunks, and/or a mesh
- One VLAN (If a VLAN is already assigned to a mirroring session, assigning another VLAN to the same session causes the second assignment to overwrite the first.)
- One ACL assignment per session (For example, if you configure an ACL as the source for mirrored traffic inbound on VLAN 1 for session 4, no port, trunk, mesh, other ACL, or other VLAN mirroring sources can be configured for session 4.)
- Up to 320 MAC addresses (used to select traffic according to source and/or destination MAC address) in all mirroring sessions configured on a switch

Using Interface Identity and Direction of Movement To Select the Traffic To Mirror from a Source Switch

Use the commands in this section to configure mirrored traffic selection for either local or remote mirroring. Options for the selection criteria includes:

- Interface Options: VLAN, port, or trunk
- Directional Options: entering or leaving the switch, or both

Port, Trunk, and/or Mesh Interface with Traffic Direction as the Selection Criteria. Use this command when the direction of traffic movement on the port, trunk, and/or mesh interface defines the criteria for mirroring traffic.

Syntax: [no] interface < *port/trunk/mesh* > monitor all < in | out | both > mirror
< 1 - 4 | *name-str* > [< 1 - 4 | *name-str* > < 1 - 4 | *name-str* >
< 1 - 4 | *name-str* >]

This command assigns a mirroring source to a previously configured mirroring session on a source switch. It specifies the port. trunk, and/or mesh source(s) to use, the direction of traffic to mirror, and the session identifier.

The **no** *form of the command removes a mirroring source assigned to the session, but does not remove the session itself. This enables you to repurpose a session by removing an unwanted mirroring source and adding another in its place.*

interface < ***port/trunk/mesh*** **>**: *Identifies the port(s), static trunk(s), and/or mesh on which to mirroring traffic. Use a hyphen for a range of consecutive ports or trunks (* `a5-a8`, `Trk2-Trk4`). *Use a comma to separate non-contiguous interfaces (*`b11,b14,Trk4,Trk7`*).*

monitor all < in | out | both >: *For the interface specified by* **<** ***port/trunk/mesh*** **>**, *selects traffic to mirror based on whether the traffic is entering or leaving the switch on the interface.*

in: *Mirror entering traffic.*

out: *Mirror exiting traffic.*

both: *Mirror traffic entering or exiting.*

(Using **monitor** *without mirroring criteria or session number affects session 1. Refer to "Monitor Command" on page B-76.)*

—Continued—

— Continued from Preceding Page—

mirror < 1 - 4 | < ***name-str*** **>**: *Assigns the traffic defined by the interface and direction to a session by number or (if configured) by name. (The session must have been previously configured. Refer to "3. Configure the Mirroring Session on the Source Switch" on page B-46.) Depending on how many sessions are already configured on the switch, you can use the same command to assign the specified source to up to four numeric or alphanumeric identifiers. For example,* `1 2 4`*. For limits on configuring mirroring sources to a given session, refer to "Mirroring Source Limits" on page B-49.*

> **< 1 - 4 > :** *Assigns a numeric session identifier to associate with the traffic selected for mirroring by this command.*
>
> **[name < name-str >]:** *Optional; uses a previously configured alphanumeric identifier to associate the traffic source with the mirroring session. The string can be used interchangeably with the mirroring session number when using this command to assign a mirroring source to a session. To configure an alphanumeric name for a mirroring session refer to the command description under "Configuring a Source Switch for a Mirroring Destination on a Remote Switch" on page B-47.*

VLAN Interface with Traffic Direction as the Selection Criteria. Use this command when the direction of traffic movement on a specific VLAN interface defines the criteria for mirroring traffic.:

Syntax: vlan < *vid-#* > monitor all < in | out | both > mirror < 1 - 4 | *name-str* >
[< 1 - 4 | *name-str* > < 1 - 4 | *name-str* > < 1 - 4 | *name-str* >]

This command assigns a mirroring source to a previously configured mirroring session on a source switch. It specifies the VLAN source to use, the direction of traffic to mirror, and the session identifier.

Assigning a VLAN to a mirroring session precludes assigning any other mirroring sources to the same session. If a VLAN is already assigned to a given mirroring session, using this command to assign another VLAN to the same mirroring session results in the second assignment replacing the first. Also, if there are other (port, trunk, or mesh) mirroring sources already assigned to a session, the switch displays a message similar to:

```
Mirror source port exists on session N. Can not
add mirror source VLAN.
```

The **no** *form of the command removes a mirroring source assigned to the session, but does not remove the session itself. This enables you to repurpose a session by removing an unwanted mirroring source and adding another in its place.*

vlan < ***vid-#*****>:** *Identifies the VLAN on which to mirror traffic.*

monitor all < in | out | both >: *Uses the traffic's direction of movement on the specified* **vid-#** *to select traffic to mirror. Refer to the syntax description on page B-50. (Using* **monitor** *without mirroring criteria or session number affects session 1. Refer to "Monitor Command" on page B-76.)*

mirror < 1 - 4 | < ***name-str*** **>**: *Assigns the traffic defined by the interface and direction to a session, by number or (if configured) by name. (The session must have been previously configured. Refer to "3. Configure the Mirroring Session on the Source Switch" on page B-46.) Depending on how many sessions are already configured on the switch, you can use the same command to assign the specified source to up to four numeric or alphanumeric identifiers. For example,* `1 2 4`*. For limits on configuring mirroring sources to a given session, refer to "Mirroring Source Limits" on page B-49.*

< 1 - 4 > : *Assigns a numeric session identifier to associate with the traffic selected for mirroring.*

— Continued —

— Continued from Preceding Page—

[name < name-str >]: *Optional; uses a previously configured alphanumeric identifier to associate the traffic source with the mirroring session. The string can be used interchangeably with the mirroring session number when using this command to assign a mirroring source to a session. To configure an alphanumeric name for a mirroring session refer to the command description under "Configuring a Source Switch for a Mirroring Destination on a Remote Switch" on page B-47.*

Using ACL Assignment and Traffic Direction To Select the Traffic To Mirror from a Source Switch

Use the commands in this section to apply ACL criteria for either local or remote mirroring.

ACL Operation for Mirroring Applications. Using the ACL (Access Control List) mirroring option requires configuration of an ACL. For ACL configuration and operating details, refer to the chapter titled "Access Control Lists (ACLs)" in the latest *Access Security Guide* for your switch.

ACLs used for selecting traffic to mirror are configured in the same way as ACLs for traffic filtering. This means that an ACL applied as a static port ACL, VLAN ACL (VACL), or routed ACL (RACL) can be applied to mirroring. (An ACL used for mirroring does not filter traffic.)

When an ACL is applied to mirroring, the **permit** and **deny** statements in the ACL take on a different role than in ACL traffic filtering. That is, a packet matching a **permit** statement will be mirrored, and a packet matching a **deny** statement (including the explicit **deny** at the end of every ACL) will not be mirrored. Any **log** keywords in ACL deny statements are ignored by the mirroring function. If both a mirrored ACL and a statically-configured ACL are applied to the same interface, and a packet matches a **permit** statement in the mirrored ACL and a **deny** statement in statically-configured ACL, the packet will be mirrored and dropped. Note that each mirrored ACL applied to an interface uses shared switch resources. The rules applicable for adding, removing, replacing, or modifying a traffic-filtering ACL also apply to an ACL used for mirroring.

Notes

If a mirroring session is configured with a mirroring source that uses an ACL for traffic selection, then no other mirroring sources can be configured to use that session. Conversely, if a mirroring session is already configured with a mirroring source that does not use an ACL, then the session cannot accept an additional mirroring source that does use an ACL.

The ACL option applies only to *IP traffic* entering the switch on the specified interface. An ACL used for mirroring purposes ignores non-IP traffic when selecting traffic to mirror.

The switch ignores any **log** statements included in **deny** ACEs in an ACL used for mirroring purposes.

ACL (Access Control List) Selection Criteria for Mirroring from a Port, Trunk, or Mesh Interface. ACL traffic filtering for mirroring purposes operates as described in the ACL chapter except that the effect of the ACL is to mirror or not mirror IP traffic, instead of to permit or deny the IP traffic.

Syntax: [no] interface <*port/trunk/mesh* > monitor ip access-group <*acl-name*> in mirror < 1 - 4 | name-str > [< 1 - 4 | name-str >] [< 1 - 4 | name-str >] [< 1 - 4 | name-str >]

This command assigns a mirroring source to a previously configured mirroring session on a source switch. It specifies the port. trunk, and/or mesh source(s) to use, the (previously configured) ACL to use for selecting traffic to mirror, and the session identifier. Use this option to mirror selected IP traffic entering the switch on specified ports, trunks, and/or a mesh.

The **no** *form of the command removes the mirroring source assigned to the session, but does not remove the session itself. This enables you to repurpose a a session by removing an unwanted mirroring source and adding another in its place.*

< interface *port/trunk/mesh* >: *Configures one or more ports, static trunks, and/or mesh on which inbound traffic is filtered and mirrored by the specified ACL. To enter consecutive ports or trunks, use a hyphen to specify the range; for example,* `a5-a8` *and* `Trk2-Trk4`. *Use a comma to separate non-contiguous interfaces (*`b11,b14,Trk4,Trk7`*).*

—Continued—

— Continued from Preceding Page—

monitor ip access-group < *acl-name* > in: *For the interface specified by* **< *port/trunk/mesh* >**, *selects the IP traffic to mirror based on the selection criteria specified in the named ACL. (The ACL must be already configured on the switch. Refer to "ACL Operation for Mirroring Applications" on page B-53.)*

(Using **monitor** *without mirroring criteria or session number affects session 1. Refer to "Monitor Command" on page B-76.)*

> **< *acl-name* >**: *For traffic entering the switch on the specified interface, mirror the IP traffic having a match with the* **permit** *ACEs in the named ACL. (IP traffic having a match with a* **deny** *ACE, including the implicit* **deny any** *or* **deny any any** *in the named ACL, will not be mirrored.)*

mirror < 1 - 4 | < *name-str* >: *Assigns the traffic defined by the interface to a session by number or (if configured) by name. (The session must have been previously configured. Refer to "3. Configure the Mirroring Session on the Source Switch" on page B-46.) Depending on how many sessions are already configured on the switch, you can use the same command to assign the specified source to up to four numeric or alphanumeric identifiers. For example,* `1 2 4`*. For limits on configuring mirroring sources to a given session, refer to "Mirroring Source Limits" on page B-49.*

> **< 1 - 4 > :** *Assigns a numeric session identifier to associate with the traffic selected for mirroring by this command.*
>
> **[name < name-str >]:** *Optional; uses a previously configured alphanumeric identifier to associate the traffic source with the mirroring session. The string can be used interchangeably with the mirroring session number when using this command to assign a mirroring source to a session. To configure an alphanumeric name for a mirroring session refer to the command description under "Configuring a Source Switch for a Mirroring Destination on a Remote Switch" on page B-47.*

ACL (Access Control List) Selection Criteria for Mirroring from a VLAN Interface.

Syntax: vlan < *vid-#* > monitor ip access-group < *acl-name* > in
mirror < 1 - 4 | name-str > [< 1 - 4 | name-str >] [< 1 - 4 | name-str >]
[< 1 - 4 | name-str >]

This command assigns a mirroring source to a previously configured mirroring session on a source switch. It specifies the VLAN source to use, the (previously configured) ACL to use for selecting traffic to mirror, and the session identifier. Use this option when you want to mirror selected IP traffic entering the switch on a specific VLAN.

The **no** *form of the command removes the mirroring source assigned to the session, but does not remove the session itself. This enables you to repurpose a a session by removing an unwanted mirroring source and adding another in its place.*

< vlan *vid-#*>: *Configures the VLAN on which inbound traffic is filtered and mirrored by the specified ACL.*

monitor ip access-group < *acl-name* > in: *For the interface specified by* **< vid-#>**, *selects the IP traffic to mirror based on the selection criteria specified in the named ACL. (The ACL must be already be configured on the switch. Refer to "ACL Operation for Mirroring Applications" on page B-53.)*

(Using **monitor** *without mirroring criteria or session number affects session 1. Refer to "Monitor Command" on page B-76.)*

< *acl-name* >: *For traffic entering the switch on the specified interface, mirror the IP traffic having a match with the* **permit** *ACEs in the named ACL. (IP traffic matching a* **deny** *ACE, including the implicit* **deny any** *or* **deny any any** *in the named ACL is dropped.)*

— Continued—

— Continued from Previous Page—

mirror < 1 - 4 | < *name-str* >: *Assigns the traffic defined by the interface to a session by number or (if configured) by name. (The session must have been previously configured. Refer to "3. Configure the Mirroring Session on the Source Switch" on page B-46.) Depending on how many sessions are already configured, you can use the same command to assign the specified source to up to four numeric or alphanumeric identifiers. For example,* `1 2 test-mirror`. *For limits on configuring mirroring sources to a given session, see "Mirroring Source Limits" on page B-49.*

> **< 1 - 4 >:** *Assigns a numeric session identifier to associate with the traffic selected for mirroring.*
>
> **[name < name-str >]:** *Optional; uses a previously configured alphanumeric identifier to associate the traffic source with the mirroring session. The string can be used interchangeably with the mirroring session number when using this command to assign a mirroring source to a session. To configure an alphanumeric name for a mirroring session refer to the command description under "Configuring a Source Switch for a Mirroring Destination on a Remote Switch" on page B-47.*

Using a MAC Address as Mirroring Criteria

Use the **monitor mac mirror** command at the global configuration level to apply a source and/or destination MAC address as the selection criteria used in a local or remote mirroring session.

While ACL-based mirroring allows you to mirror traffic using an ACL to specify IP addresses as selection criteria, MAC-based mirroring allows you monitor switch traffic using a source and/or destination MAC address. You can apply MAC-based mirroring in one or more mirroring sessions on the switch to monitor:

- Inbound traffic
- Outbound traffic
- Both inbound and outbound traffic

MAC-based mirroring is useful in ProCurve Network Immunity security solutions that provide detection and response to malicious traffic at the network edge. After isolating a malicious MAC address, a security administrator can mirror all traffic sent to, and received from, the suspicious address for troubleshooting and traffic analysis.

The MAC address that you enter with the **monitor mac mirror** command is configured to select traffic for mirroring from all ports and learned VLANs on the switch. Therefore, a suspicions MAC address used in wireless applications can be continuously monitored as it re-appears in switch traffic on different ports or VLAN interfaces.

You can configure MAC-based mirroring from the CLI or an SNMP management station and use it to mirror:

- All inbound and outbound traffic from a group of hosts to one destination device.
- Inbound and/or outbound traffic from each host to a different destination device.
- Inbound and outbound traffic from all monitored hosts separately on two destination devices: mirroring all inbound traffic to one device and all outbound traffic to another device.

To configure a MAC address to filter mirrored traffic on an interface, enter the **monitor mac mirror** command at the global configuration level.

Syntax: [no] monitor mac <*mac-addr*> <src | dest | both> mirror < 1 - 4 | name-str > [< 1 - 4 | name-str >] [< 1 - 4 | name-str >] [< 1 - 4 | name-str >]

*Use this command to configure a source and/or destination MAC address as criteria for selecting traffic in one or more mirroring sessions on the switch. The MAC address you enter is configured to mirror inbound (***src***), outbound (***dest***), or both inbound and outbound (***both***) traffic on any port or learned VLAN on the switch.*

Packets that are sent or received on an interface configured with a mirroring session and contain the MAC address as source and/or destination address are mirrored to a previously configured destination device.

To remove a MAC address as selection criteria in a mirroring session, you must enter the complete command syntax; for example, **no monitor mac 998877-665544 dest mirror 4**.

The **no** *form of the command removes the MAC address as a mirroring criteria from an active session, but does not remove the session itself. This enables you to repurpose a a session by removing an unwanted mirroring criteria and adding another in its place.*

monitor mac < ***mac-addr*** **>**: *Configures the MAC address as selection criteria for mirroring traffic on any port or learned VLAN on the switch.*

—Continued—

— Continued from Preceding Page—

< src | dest | both >: *Specifies how the MAC address is used to filter and mirror packets in inbound and/or outbound traffic on the interfaces on which the mirroring session is applied:*

src*: Mirrors all packets in inbound traffic that contain the specified MAC address as source address.*

dest*: Mirrors all packets in outbound traffic that contain the specified MAC address as destination address.*

Note: *The MAC address of the switch is not supported as either the source or destination MAC address used to select mirrored traffic.*

both*: Mirrors all packets in both inbound and outbound traffic that contain the specified MAC address as either source or destination address.*

mirror < 1 - 4 | < ***name-str*** **>**: *Assigns the inbound and/or outbound traffic filtered by the specified MAC address to a previously configured mirroring session. The session is identified by a number or (if configured) a name.*

Depending on how many sessions are configured on the switch, you can use the same command to configure a MAC address as mirroring criteria in up to four sessions. To identify a session, you can enter either its name or number; for example: **mirror 1 2 3 traffsrc4**

Refer to "Mirroring Source Limits" on page B-49 for the restrictions on how many mirroring source criteria you can configure in the same session.

> **< 1 - 4 >:** *Specifies a mirroring session by number (1 to 4), for which the configured MAC address is used to select and mirror inbound and/or outbound traffic.*
>
> **[name < name-str >]:** *(Optional) Specifies a mirroring session by name (alphanumeric string), for which the configured MAC address is used to select and mirror inbound and/or outbound traffic. For a remote mirroring session, you must configure the same session name on both the source and destination switch.*

Restrictions

The following restrictions apply to MAC-based mirroring:

- Up to 320 different MAC addresses are supported for traffic selection in all mirroring sessions configured on the switch.
- A destination MAC address is not supported as mirroring criteria for routed traffic because in routed packets, the destination MAC address is changed to the next-hop address when the packet is forwarded. Therefore, the destination MAC address that you want to mirror will not appear in routed packet headers.

  This restriction also applies to the destination MAC address of a host that is directly connected to a routing switch. (Normally, a host is connected to an edge switch, which is directly connected to the router.)

  To mirror routed traffic, it is recommended that you use IP-based ACLs to select traffic for mirroring as described in "Using ACL Assignment and Traffic Direction To Select the Traffic To Mirror from a Source Switch" on page B-53.
- On a switch, you can use a MAC address only once as a source MAC address, and only once as a destination MAC address, to filter mirrored traffic.

  For example, after you enter the following commands:
  monitor mac 111111-222222 src mirror 1
  monitor mac 111111-222222 dest mirror 2

  The following commands are not supported:
  monitor mac 111111-222222 src mirror 3
  monitor mac 111111-222222 dest mirror 4

  In addition, if you enter the **monitor mac 111111-222222 both mirror 1** command, you cannot use the MAC address **111111-222222** in any other **monitor mac mirror** configuration commands on the switch.
- To re-use a MAC address that has already been configured as a source and/or destination address for traffic selection in a mirror session, you must first remove the configuration by entering the **no** form of the command, and then re-enter the MAC address in a new **monitor mac mirror** command.

  For example, if you have already configured MAC address **111111-222222** to filter inbound and outbound mirrored traffic, and decide to use it to filter only inbound traffic in a mirror session, you could enter the following commands:
  monitor mac 111111-222222 both mirror 1
  no monitor mac 111111-222222 both mirror 1
  monitor mac 111111-222222 src mirror 1

- A mirroring session in which you configure MAC-based mirroring is not supported on a port, trunk, mesh or VLAN interface on which a mirroring session with ACL-based mirroring is configured.

Displaying the Mirroring Configuration

Displaying the Mirroring Configuration Summary

Use the **show monitor** command to display summary information on the current source and destination mirroring configured on the switch.

Syntax: show monitor

If a remote mirroring source is configured on the switch, then the following fields appear. Otherwise, the output displays this message: **Mirroring is currently disabled**.

Sessions: *Lists the four configurable sessions on the switch.*

Status: *Displays the current status of each session:*

active: *The session is configured.*

inactive: *The session is partially configured. Only the destination has been configured; the mirroring source is not configured.*

not defined: *Mirroring is not configured for this session.*

Type: *Indicates whether the mirroring session is local (***port***), remote (***IPv4***), or MAC-based (***mac***) for local or remote sessions.*

Sources: *Indicates how many mirroring sources are using each mirroring session.*

ACL: *Indicates whether the source is using an ACL to select traffic for mirroring.*

If a remote mirroring endpoint is configured on the switch, then the following fields appear. Otherwise, the output displays the following: **There are no Remote Mirroring endpoints currently assigned**.

Type: *Indicates whether the mirroring session is local (***port***), remote (***IPv4***), or MAC-based (***mac***) for local or remote sessions.*

UDP Source Addr: *The IP address configured for the source VLAN or subnet on which the traffic source exists. (For a given mirroring session, this value should be the same on the source and destination switches.)*

—Continued—

Syntax: show monitor

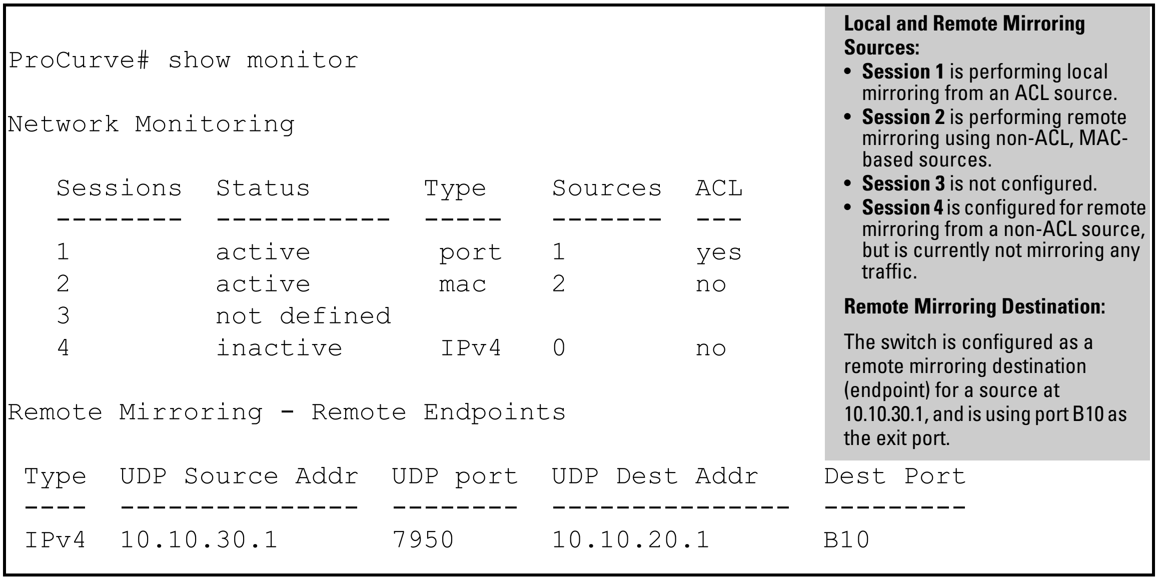
—Continued from Previous Page—

UDP port: *The unique UDP port number identifying a given mirroring session. (For a given mirroring session, this value should be the same on the source and destination switches.)*

UDP Dest Addr: *The IP address configured as the destination VLAN or subnet on which the exit port exists. (For a given mirroring session, this value should be the same on the source and destination switches.)*

Dest Port: *For a given mirroring session, identifies the exit port on the destination switch.*

For example, the following summary shows three mirroring sources (one local and two remote) and one remote mirroring destination configured on the switch.



```
ProCurve# show monitor

Network Monitoring

   Sessions  Status       Type    Sources  ACL
   --------  -----------  -----   -------  ---
   1         active        port   1        yes
   2         active        mac    2        no
   3         not defined
   4         inactive      IPv4   0        no

Remote Mirroring - Remote Endpoints

 Type  UDP Source Addr  UDP port  UDP Dest Addr    Dest Port
 ----  ---------------  --------  ---------------  ---------
 IPv4  10.10.30.1       7950      10.10.20.1       B10
```

Local and Remote Mirroring Sources:

- **Session 1** is performing local mirroring from an ACL source.
- **Session 2** is performing remote mirroring using non-ACL, MAC-based sources.
- **Session 3** is not configured.
- **Session 4** is configured for remote mirroring from a non-ACL source, but is currently not mirroring any traffic.

Remote Mirroring Destination:

The switch is configured as a remote mirroring destination (endpoint) for a source at 10.10.30.1, and is using port B10 as the exit port.

Figure B-22. Example of a Currently Configured Mirroring Summary on a Source Switch

Displaying the Remote Endpoint Configuration

Syntax: show monitor endpoint

This command displays the remote mirroring endpoint configuration on a switch. It does not include information for any local mirroring sessions configured on the switch. (To view a local mirroring configuration on the switch, use **show monitor [< 1-4 | name < name-str >]***; pages B-61 and B-64.)*

Type: *Indicates whether the session is a* **port** *(local) or* **IPv4** *(remote) mirroring session.*

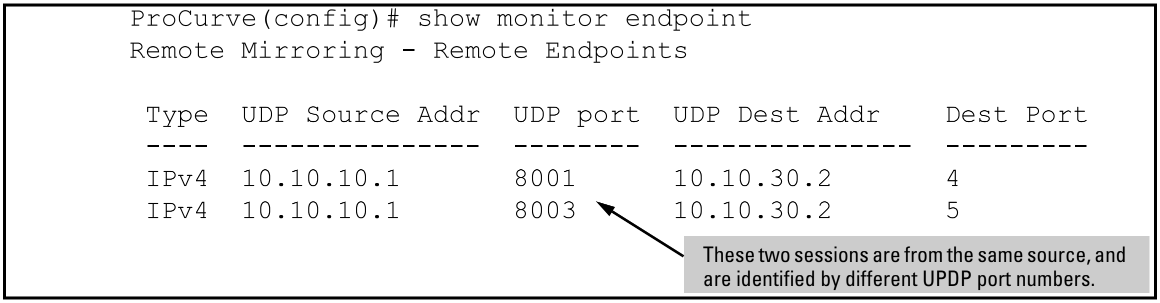
UDP Source Addr: *The IP address configured as the source VLAN or subnet on which the traffic source exists. (For a given mirroring session, this value should be the same on the source and destination switches.)*

UDP port: *The unique UDP port number identifying a given mirroring session. (For a given mirroring session, this value should be the same on the source and destination switches.)*

UDP Dest Addr: *The IP address configured as the destination VLAN or subnet on which the exit port exists. (For a given mirroring session, this value should be the same on the source and destination switches.)*

Dest Port: *For a given mirroring session, identifies the exit port on the destination switch.*

For example, the following output indicates that a switch is configured as the endpoint (destination) for two remote mirroring sessions from the same source.



```
ProCurve(config)# show monitor endpoint
Remote Mirroring - Remote Endpoints

 Type  UDP Source Addr  UDP port  UDP Dest Addr    Dest Port
 ----  ---------------  --------  ---------------  ---------
 IPv4  10.10.10.1       8001      10.10.30.2       4
 IPv4  10.10.10.1       8003      10.10.30.2       5
```

These two sessions are from the same source, and are identified by different UPDP port numbers.

Figure B-23. Example of Displaying Only the Mirroring Endpoint Configuration

Displaying a Mirroring Session Configuration on a Source Switch

Syntax: show monitor < 1 - 4 | name < *name-str* >

Use this command to display detailed configuration information on the specified local or remote mirroring session on a source switch.

Session: *Displays the numeric ID of the selected session.*

Session Name: *Displays the alphanumeric name of the session, if configured.*

ACL: *Indicates whether the source is using an ACL to select traffic for mirroring.*

Mirroring Destination: *For a local mirroring session, indicates the port configured as the exit port on the source switch. For a remote mirroring session, shows* **IPv4**, *which indicates mirroring to a remote (exit) switch.*

UDP Source Addr: *The IP address configured for the source VLAN or subnet on which the traffic source exists. (For a given mirroring session, this value should be the same on the source and destination switches.)*

UDP port: *The unique UDP port number identifying a given mirroring session. (For a given mirroring session, this value should be the same on the source and destination switches.)*

UDP Dest Addr: *The IP address configured as the destination VLAN or subnet on which the exit port exists. (For a given mirroring session, this value should be the same on the source and destination switches.)*

Status: *For a remote monitoring session, displays current session activity:*

active: *The session is configured and is mirroring traffic. A remote path has been discovered to the destination.*

inactive: *The session is configured, but is not currently mirroring traffic. A remote path has not been discovered to the destination.*

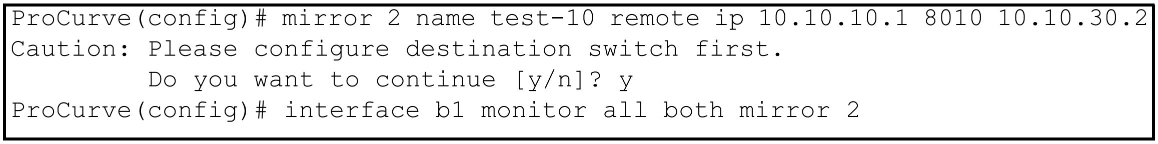
not defined: *Mirroring is not configured for this session.*

Monitoring Sources: *For the specified local or remote session, displays the source (port, trunk, or VLAN) interface and the MAC address (if configured) used to select mirrored traffic.*

Syntax: show monitor < 1 - 4 | name < *name-str* >

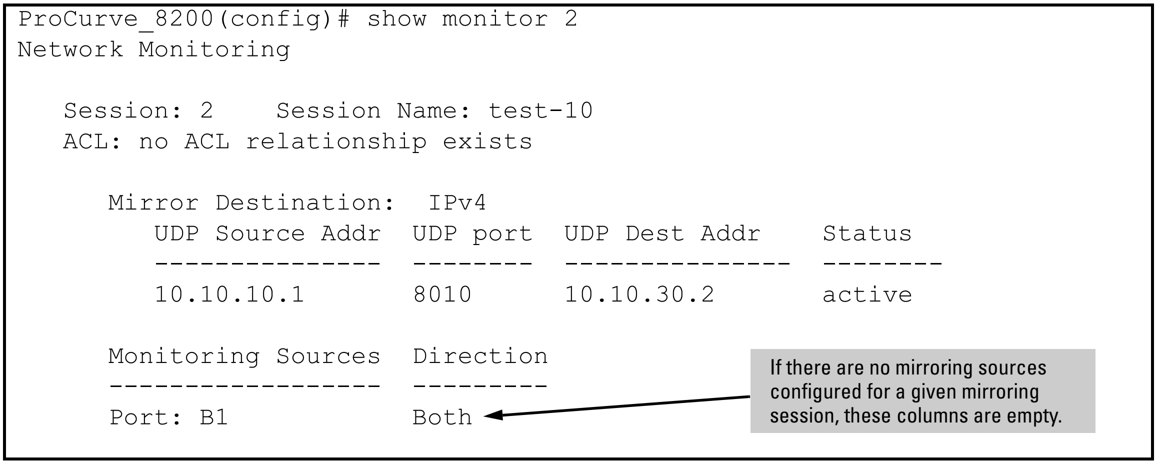
Direction: *For the selected interface, indicates whether mirrored traffic is entering the switch (***in***), leaving the switch (***out***), or* **both**.

Example: Remote Mirroring Session. If you configure remote mirroring session 2 as shown in Figure B-24, you can enter the **show monitor 2** command to verify the configuration (see Figure B-25).



```
ProCurve(config)# mirror 2 name test-10 remote ip 10.10.10.1 8010 10.10.30.2
Caution: Please configure destination switch first.
         Do you want to continue [y/n]? y
ProCurve(config)# interface b1 monitor all both mirror 2
```

Figure B-24. Example of Configuring a Remote Mirroring Session and Corresponding Source

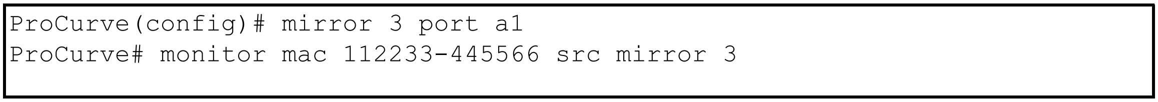


```
ProCurve_8200(config)# show monitor 2
Network Monitoring

   Session: 2    Session Name: test-10
   ACL: no ACL relationship exists

      Mirror Destination:  IPv4
         UDP Source Addr  UDP port  UDP Dest Addr    Status
         ---------------  --------  ---------------  --------
         10.10.10.1       8010      10.10.30.2       active

      Monitoring Sources  Direction
      ------------------  ---------
      Port: B1            Both
```

If there are no mirroring sources configured for a given mirroring session, these columns are empty.

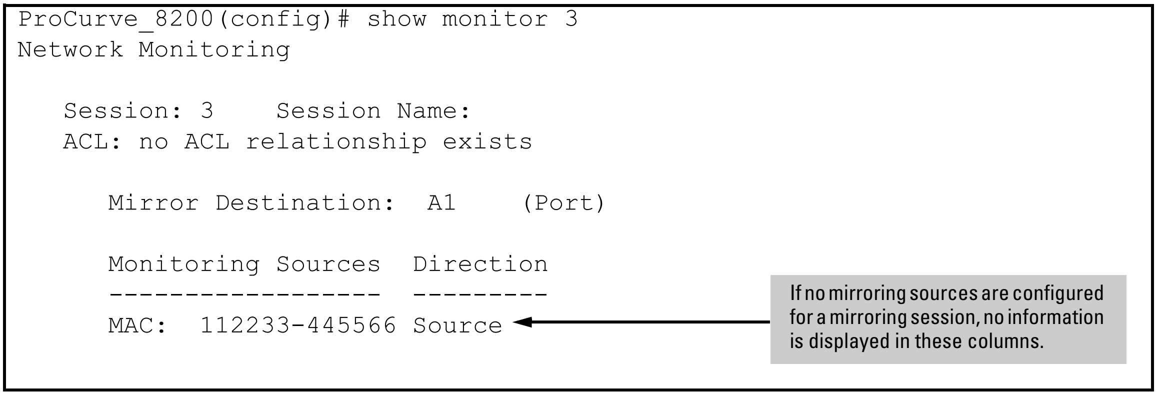
Figure B-25. Example of Verifying the Configuration of a Remote Mirroring Session

Example: MAC-based Mirroring Session. If you configure a MAC-based mirroring session as shown in Figure B-26, you can enter the **show monitor 3** to display the configuration (see Figure B-27).



```
ProCurve(config)# mirror 3 port a1
ProCurve# monitor mac 112233-445566 src mirror 3
```

Figure B-26. Example of Configuring a MAC-based Mirroring Session



```
ProCurve_8200(config)# show monitor 3
Network Monitoring

   Session: 3    Session Name:
   ACL: no ACL relationship exists

      Mirror Destination:  A1    (Port)

      Monitoring Sources  Direction
      ------------------  ---------
      MAC:  112233-445566 Source
```

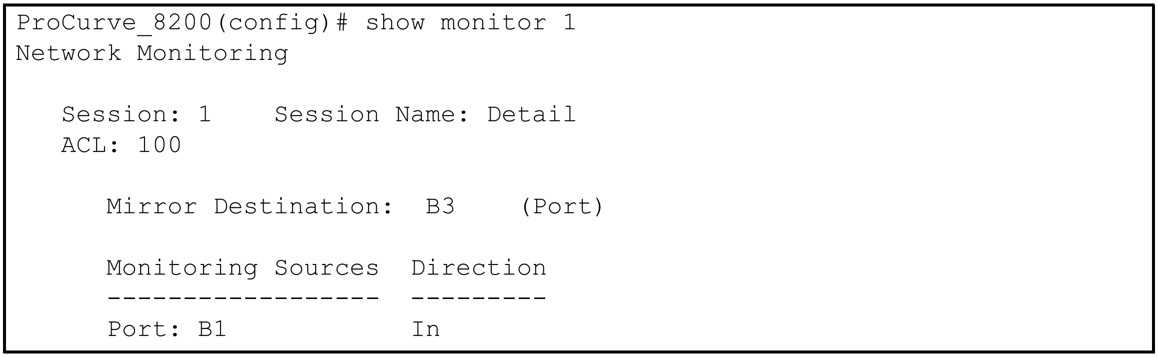
If no mirroring sources are configured for a mirroring session, no information is displayed in these columns.

Figure B-27. Example of Verifying the a MAC-based Mirroring Session

If the selected session is configured for local mirroring, using **show monitor** with the session number displays a subset of the types of information displayed for a remote mirroring session. For example, suppose a session is configured as follows for local mirroring:

- Use "1" as the session number.
- Use "Detail" as the session name.
- Use ACL 100 (previously configured on the switch) to mirror the inbound traffic on port B1.
- Send the mirrored traffic to (exit) port B3.

For the above configuration, **show monitor 1** produces the following output:



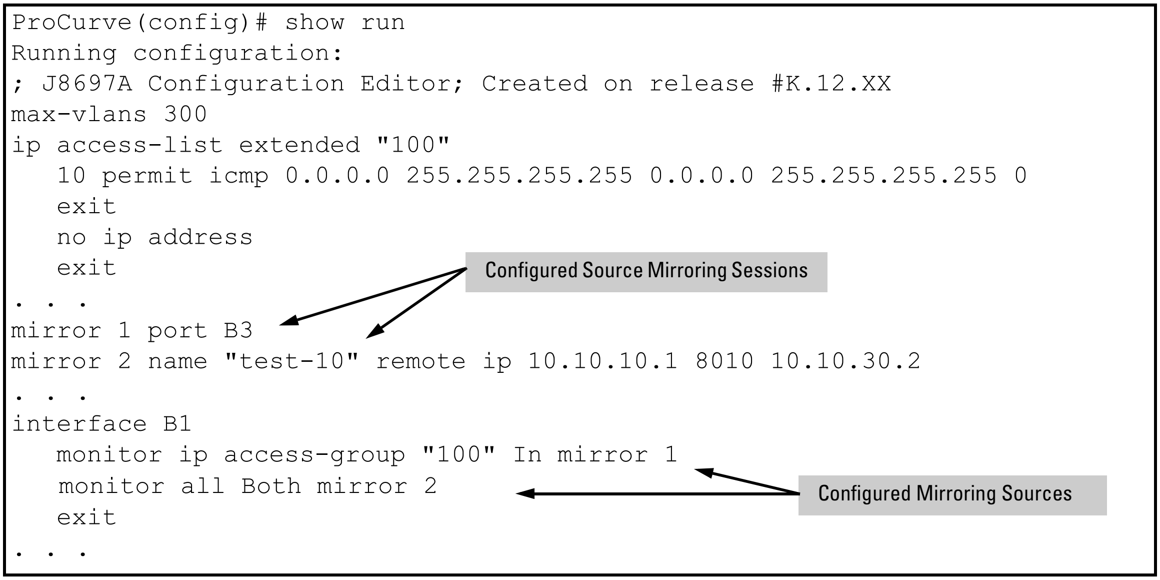
```
ProCurve_8200(config)# show monitor 1
Network Monitoring

   Session: 1    Session Name: Detail
   ACL: 100

      Mirror Destination:  B3    (Port)

      Monitoring Sources  Direction
      ------------------  ---------
      Port: B1            In
```

Figure B-28. Example of Output for a Local Mirroring Session

Viewing Mirroring in the Current Configuration File

Using the **show run** command, you can view the current mirroring configuration on the switch.

Source mirroring session entries begin with the **mirror** keyword and the mirroring sources are listed per-interface. For example:

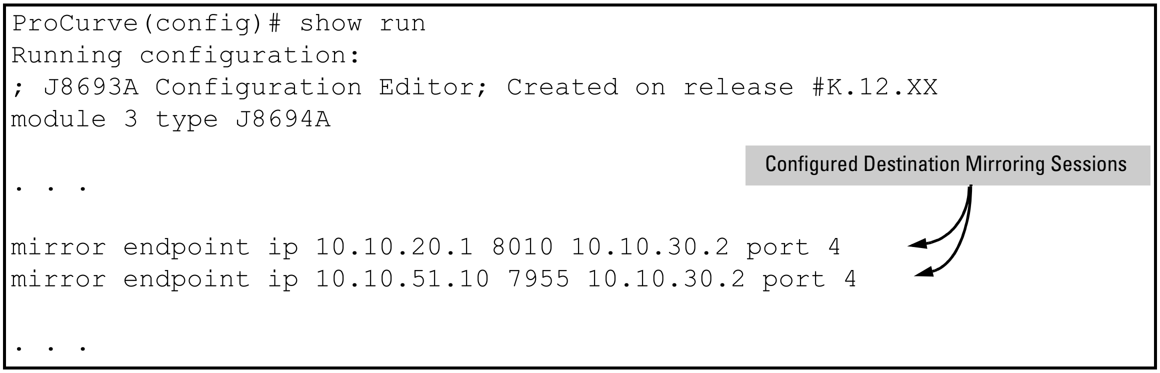


```
ProCurve(config)# show run
Running configuration:
; J8697A Configuration Editor; Created on release #K.12.XX
max-vlans 300
ip access-list extended "100"
   10 permit icmp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 0
   exit
   no ip address
   exit
. . .
mirror 1 port B3
mirror 2 name "test-10" remote ip 10.10.10.1 8010 10.10.30.2
. . .
interface B1
   monitor ip access-group "100" In mirror 1
   monitor all Both mirror 2
   exit
. . .
```

Configured Source Mirroring Sessions
Configured Mirroring Sources

Figure B-29. Example of Using the Configuration File to View the Source Mirroring Configuration

Destination mirroring session entries begin with **mirror endpoint**. In the following example, two sessions are using the same exit port:



```
ProCurve(config)# show run
Running configuration:
; J8693A Configuration Editor; Created on release #K.12.XX
module 3 type J8694A

. . .

mirror endpoint ip 10.10.20.1 8010 10.10.30.2 port 4
mirror endpoint ip 10.10.51.10 7955 10.10.30.2 port 4

. . .
```

Figure B-30. Example of Using the Configuration File to View the Source Mirroring Configuration

Mirroring Configuration Examples

Local Mirroring Destination

Example of Local Mirroring Configuration. A system operator wants to mirror the inbound traffic from workstation “X” on port A5 and workstation “Y” on port B17 to a traffic analyzer connected to port C24. In this case, the operator chooses “1” as the session number. (Any unused session number from 1 to 4 is valid.) Since the switch provides both the source and destination for the traffic to monitor, local mirroring can be configured. In this case, the command sequence is:

1. Configure the local mirroring session.
2. Assign a mirroring source to the session.

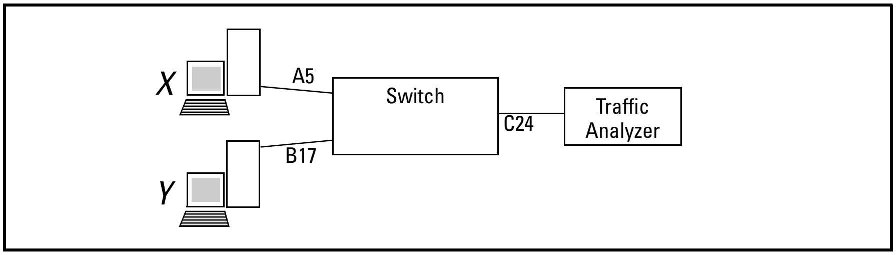
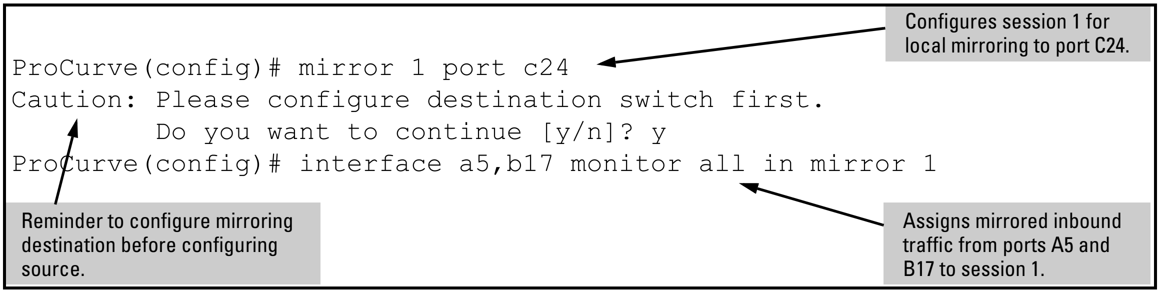


Figure B-31. Example of a Local Mirroring Topology



Configures session 1 for local mirroring to port C24.

```
ProCurve(config)# mirror 1 port c24
Caution: Please configure destination switch first.
         Do you want to continue [y/n]? y
ProCurve(config)# interface a5,b17 monitor all in mirror 1
```

Reminder to configure mirroring destination before configuring source.

Assigns mirrored inbound traffic from ports A5 and B17 to session 1.

Figure B-32. Example of Configuring Local Mirroring of Inbound Traffic

Remote Mirroring Destination Using a VLAN Interface and an ACL for Mirroring Criteria

In the network shown in figure B-33, the system operator has connected a traffic analyzer to port A15 (in VLAN 30) on switch D, and wants to monitor the Telnet traffic to the server at 10.10.30.153 from the workstations on switches A and B. The operator does this by configuring remote mirroring sessions on these two switches, and a mirroring destination on switch D. (Telnet traffic to the server from sources on switch C is not of interest, and routing is enabled on switches C and D.)

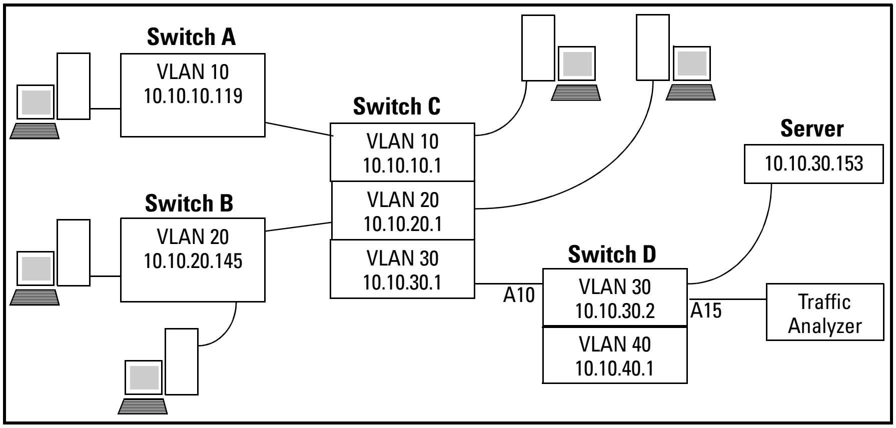
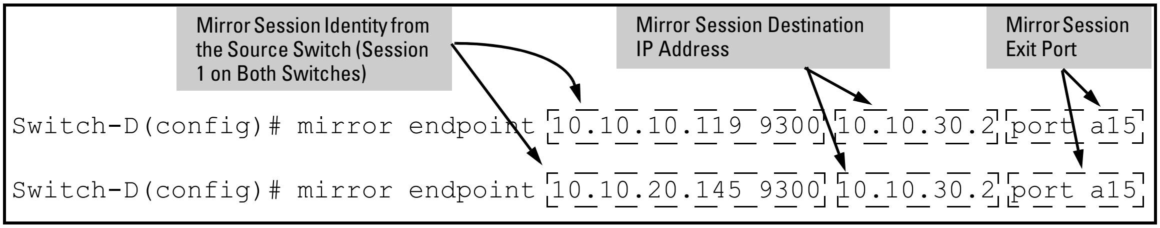


Figure B-33. Example Topology for Remote Mirroring from a VLAN Interface

The operator does the following:

1. On switch D, configure a mirroring destination using port A15 In VLAN 30 as the exit port.
2. Configure switches A and B with mirroring sessions to the destination interface on switch D. Use a randomly selected UDP port number of 9300. (For information on selecting UDP port numbers to use for remote mirroring, refer to the syntax description on page B-45.) You can use the same random UDP port number on different interfaces because the identity of the mirroring source is the combination of the unique interface identity and the UDP port number, and not the UDP port number alone.
3. Configure an ACL on switches A and B to select inbound Telnet traffic intended for the server at 10.10.30.153.
4. Using the ACLs to select the traffic to mirror, configure mirroring sessions for Telnet traffic entering switches A and B on VLANs 10 and 20. (Because the sessions are on different switches, you can use the same session number for both sessions if you want to.)

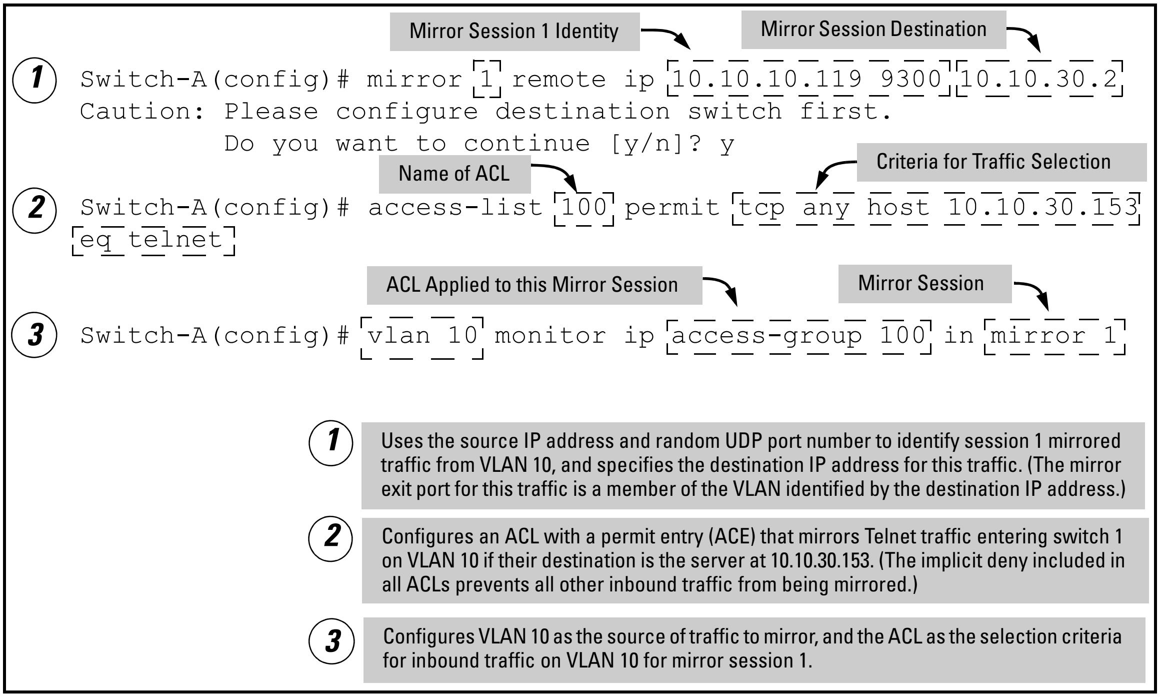
The following three figures illustrate the configuration steps on the mirroring destination switch (switch D) and on the mirroring sources (switches A and B). Since there is no need for a mirroring configuration on the intermediate device (switch C), this device can be any switch (or router) supporting IPv4 operation.



```
Switch-D(config)# mirror endpoint 10.10.10.119 9300 10.10.30.2 port a15
Switch-D(config)# mirror endpoint 10.10.20.145 9300 10.10.30.2 port a15
```

Mirror Session Identity from the Source Switch (Session 1 on Both Switches)
Mirror Session Destination IP Address
Mirror Session Exit Port

Figure B-34. Example of Configuring Remote Mirroring from Switches A and B on the Destination Switch

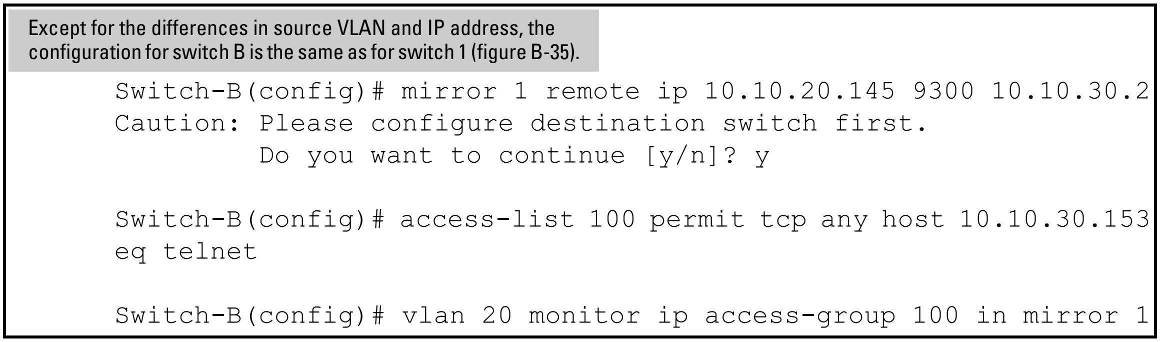


```
1  Switch-A(config)# mirror 1 remote ip 10.10.10.119 9300 10.10.30.2
   Caution: Please configure destination switch first.
            Do you want to continue [y/n]? y
2  Switch-A(config)# access-list 100 permit tcp any host 10.10.30.153
   eq telnet
3  Switch-A(config)# vlan 10 monitor ip access-group 100 in mirror 1
```

Mirror Session 1 Identity
Mirror Session Destination
Name of ACL
Criteria for Traffic Selection
ACL Applied to this Mirror Session
Mirror Session

1. Uses the source IP address and random UDP port number to identify session 1 mirrored traffic from VLAN 10, and specifies the destination IP address for this traffic. (The mirror exit port for this traffic is a member of the VLAN identified by the destination IP address.)
2. Configures an ACL with a permit entry (ACE) that mirrors Telnet traffic entering switch 1 on VLAN 10 if their destination is the server at 10.10.30.153. (The implicit deny included in all ACLs prevents all other inbound traffic from being mirrored.)
3. Configures VLAN 10 as the source of traffic to mirror, and the ACL as the selection criteria for inbound traffic on VLAN 10 for mirror session 1.

Figure B-35. Example of Configuring Remote Mirroring of Inbound Traffic on Source Switch 1



Except for the differences in source VLAN and IP address, the configuration for switch B is the same as for switch 1 (figure B-35).

```
Switch-B(config)# mirror 1 remote ip 10.10.20.145 9300 10.10.30.2
Caution: Please configure destination switch first.
         Do you want to continue [y/n]? y

Switch-B(config)# access-list 100 permit tcp any host 10.10.30.153
eq telnet

Switch-B(config)# vlan 20 monitor ip access-group 100 in mirror 1
```

Figure B-36. Example of Configuring Remote Mirroring of Inbound Traffic on Source Switch 2

Remote Mirroring Destination Using a Port Interface and Directional Mirroring Criteria

In the network shown in figure B-37, the system operator has connected another traffic analyzer to port B10 (in VLAN 40) on switch D, and wants to monitor all traffic entering Switch A from client "X" on port C12. The operator does this by configuring a mirroring destination (with an exit port of B10) on switch D, and a remote mirroring session on Switch A. For this example, assume that the mirroring configuration from the proceeding example remains in place. This means that a different mirroring session number and UDP port number will be needed. Note that the port on which the mirrored traffic for this example enters switch D, port A20, must be in the same VLAN as the configured exit port for Traffic Analyzer 2, which is port B10.

Note

Because this example and the proceeding example create remote mirroring between the same source and destination IP addresses, the random UDP port number used in this example must be different than the one used in the proceeding example.

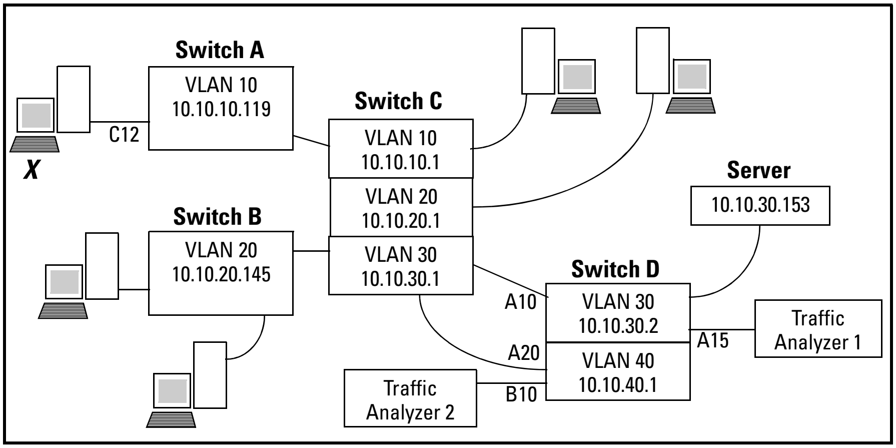


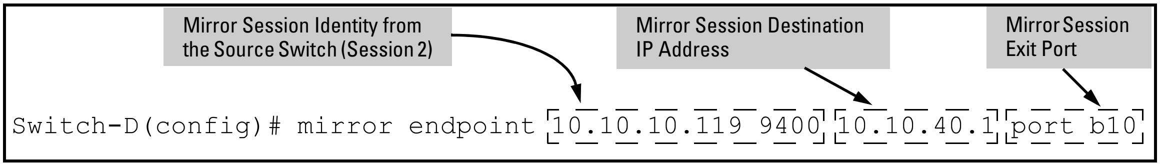
Figure B-37. Example Topology for Remote Mirroring from a Port Interface

The operator does the following:

1. On switch D, configure a mirroring destination using port B10 In VLAN 40 as the exit port.

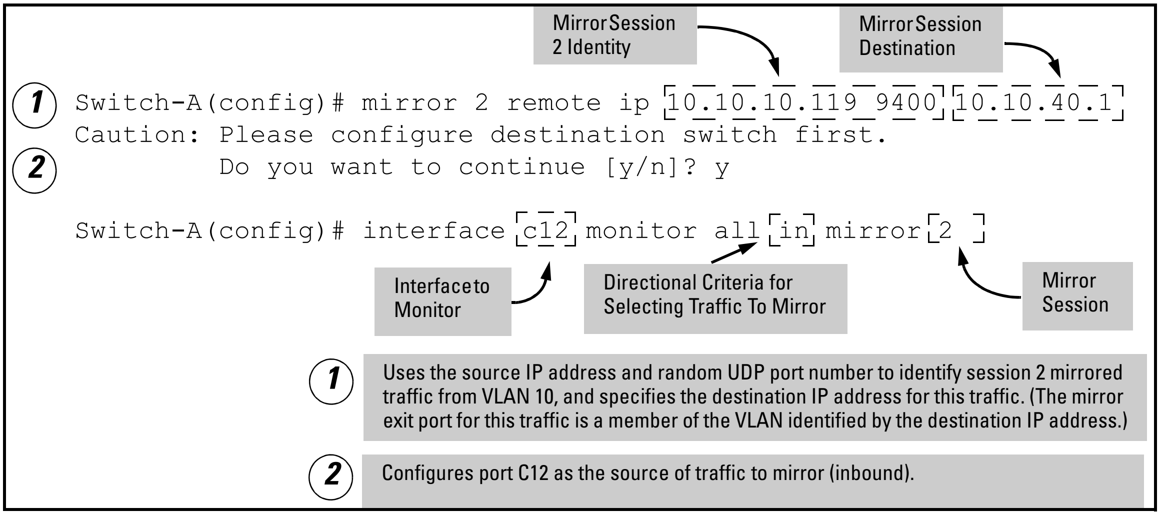
2. Using **in** to specify the traffic selection criteria, configure mirroring session 2 on switch A for port C12. (The proceeding example configured session 1 on the same switch.)

3. Configure switch A to mirror session 2 to the destination interface for port B10 on switch D. Use a randomly selected UDP port number of 9400. (Refer to the Note on page B-71.) If you need information on selecting UDP port numbers to use for remote mirroring, refer to the syntax description on page B-45.


Mirror Session Identity from
the Source Switch (Session 2)
Mirror Session Destination
IP Address
Mirror Session
Exit Port

```
Switch-D(config)# mirror endpoint 10.10.10.119 9400 10.10.40.1 port b10
```

Figure B-38. Example of Configuring Remote Mirroring for Session 2 on the Destination Switch



```
1  Switch-A(config)# mirror 2 remote ip 10.10.10.119 9400 10.10.40.1
   Caution: Please configure destination switch first.
2           Do you want to continue [y/n]? y

   Switch-A(config)# interface c12 monitor all in mirror 2
```

Mirror Session 2 Identity
Mirror Session Destination
Interface to Monitor
Directional Criteria for Selecting Traffic To Mirror
Mirror Session

1 Uses the source IP address and random UDP port number to identify session 2 mirrored traffic from VLAN 10, and specifies the destination IP address for this traffic. (The mirror exit port for this traffic is a member of the VLAN identified by the destination IP address.)

2 Configures port C12 as the source of traffic to mirror (inbound).

Figure B-39. Example of Configuring a Remote Mirroring Session for Traffic Inbound on a Port

Maximum Supported Frame Size

The IPv4 encapsulation of mirrored traffic adds a 54-byte header to each mirrored frame. If a resulting frame exceeds the MTU (Maximum Transmission Unit) allowed in the network, the frame is dropped.

Note

Mirroring does not truncate frames, and oversized mirroring frames will be dropped. Also, remote mirroring does not allow downstream devices in a mirroring path to fragment mirrored frames.

If jumbo frames are enabled on the mirroring source switch, then the mirroring destination switch and all downstream devices connecting the source switch to the mirroring destination must be configured to support jumbo frames.

Enabling Jumbo Frames To Increase the Mirroring Path MTU

On 1 Gbps and 10 Gbps ports in the mirroring path, you can reduce the number of dropped frames by enabling jumbo frames on all intermediate switches and routers. (The maximum transmission unit—MTU—on the switches covered by this manual is 9220 bytes for frames having an 802.1Q VLAN tag, and 9216 bytes for untagged frames.) For information on configuring the switch for jumbo frames, refer to “Configuring Jumbo Frame Operation” on page 13-29.

Table B-2. Maximum Frame Sizes for Mirroring

	Frame Type Configuration	Maximum Frame Size	VLAN Tag	Frame Mirrored to Local Port	Frame Mirrored to Remote Port	
				Data	Data	IPv4 Header
Untagged	Non-Jumbo (default config.)	1518	0	1518	1464	54
	Jumbo[1] on All VLANs	9216	0	9216	9162	54
	Jumbo[1] On All But Source VLAN	1518	0	n/a[2]	1464	54
Tagged	Non-Jumbo	1522	4	1522	1468	54
	Jumbo[1] on All VLANs	9220	4	9218	9164	54
	Jumbo[1] On All But Source VLAN	1522	4	n/a[2]	1468	54

[1] Jumbo frames are allowed on ports operating at or above 1 Gbps.

[2] For local mirroring, a non-Jumbo configuration on the source VLAN dictates an MTU of 1518 bytes for untagged frames, and an MTU of 1522 for tagged frames, regardless of the Jumbo configuration on any other VLANs on the switch.

Effect of Downstream VLAN Tagging on Untagged, Mirrored Traffic

In a remote mirroring application, if mirrored traffic leaves the switch without 802.1Q VLAN tagging, but is forwarded through a downstream device that adds 802.1Q VLAN tags, then the MTU for untagged, mirrored frames leaving the source switch is reduced below the values shown in table B-2. That is, if the MTU on the path to the destination is 1522 bytes, then untagged, mirrored frames leaving the source switch cannot exceed 1518 bytes. If the MTU on the path to the destination is 9220 bytes, then untagged, mirrored frames leaving the source switch cannot exceed 9216 bytes.

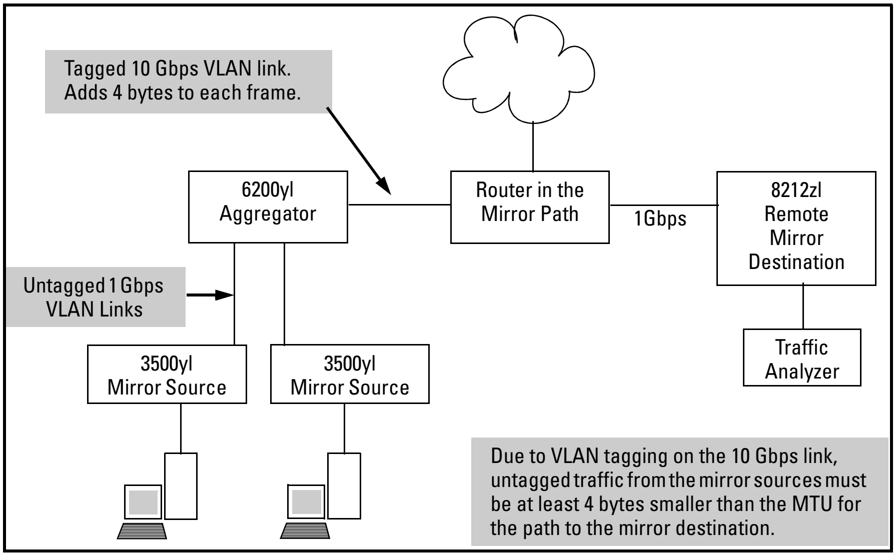

Tagged 10 Gbps VLAN link.
Adds 4 bytes to each frame.
6200yl
Aggregator
Router in the
Mirror Path
1Gbps
8212zl
Remote
Mirror
Destination
Untagged 1 Gbps
VLAN Links
Traffic
Analyzer
3500yl
Mirror Source
3500yl
Mirror Source
Due to VLAN tagging on the 10 Gbps link, untagged traffic from the mirror sources must be at least 4 bytes smaller than the MTU for the path to the mirror destination.

Figure B-40. Effect of Downstream VLAN Tagging on the MTU for Mirrored Traffic

Operating Notes

- **Mirroring Dropped Traffic:** Where an interface is configured to mirroring traffic to a destination, it does so regardless of whether the traffic is dropped while on the interface. For example, if an ACL configured on a VLAN with a **deny** ACE that eliminates packets from a Telnet application, the switch still mirrors the Telnet packets it receives on the interface and subsequently drops.
- **Mirroring and Spanning Tree:** Mirroring is done regardless of the spanning-tree (STP) state of a port or trunk. This means, for example, that inbound traffic on a port blocked by STP can still be monitored for STP protocol packets during the STP setup phase.
- **Tagged and Untagged Frames:** For a frame entering or leaving the switch on a mirrored port, the mirrored copy retains the tagged or untagged state the original frame carried when it entered into or exited from the switch. (The tagged or untagged VLAN membership of ports in the path leading to the mirroring destination does not affect the tagged or untagged status of the mirrored copy itself.) Thus, if a tagged frame arrives on a mirrored port, the mirrored copy will also be tagged, regardless of the status of ports in the destination path. If a frame exits from the switch on a mirrored port that is a tagged member of a VLAN, then the mirrored copy will also be tagged for the same reason.

- **Effect of IGMP on Mirroring:** If both inbound and outbound mirroring is operating when IGMP is enabled on any VLAN, two copies of mirrored IGMP frames may appear at the mirroring destination.
- **Mirrored Traffic Not Encrypted:** Mirrored traffic undergoes IPv4 encapsulation, but mirrored, encapsulated traffic is not encrypted.
- **IPv4 Header Added:** The IPv4 encapsulation of mirrored traffic adds a 54-byte header to each mirrored frame. If a resulting frame exceeds the maximum MTU allowed in the network, it will be dropped. To reduce the number of dropped frames, enable jumbo frames in the mirroring path, including all intermediate switches and/or routers. (The maximum transmission unit—MTU—on the switch is 9220 bytes, which includes 4 bytes for the 802.1Q VLAN tag.) For more information, refer to “Maximum Supported Frame Size” on page B-73. To configure the switch for jumbo frames, refer to “Configuring Jumbo Frame Operation” on page 13-29.
- **Intercepted or Injected Traffic:** The mirroring feature does not protect against either mirrored traffic being intercepted or traffic being injected into a mirrored stream by an intermediate host.
- **Inbound Mirrored IPv4-Encapsulated Frames are Not Mirrored:** The switch does not mirror IPv4-encapsulated mirrored frames that it receives on an interface. This prevents duplicate mirrored frames in configurations where the port connecting the switch to the network path for mirroring to a destination is also a port whose inbound or outbound traffic is being mirrored. For example, if traffic leaving the switch through ports B5, B6, and B7 is being mirrored through port B7 to a network analyzer, the mirrored frames from traffic on ports B5 and B6 will not be mirrored a second time as they pass through port B7.
- **Switch Operation as Both Destination and Source:** A switch configured as remote destination switch can also be configured to mirror traffic to one of its own ports (local mirroring) or to a destination on another switch (remote mirroring).
- **Monitor Command Note:** If session 1 is already configured with a destination, you can execute **[no] vlan < vid > monitor** or **[no] interface < port > monitor** without mirroring criteria and a mirror session number. In this case, the switch automatically configures or removes mirroring for inbound and outbound traffic from the specified VLAN or port(s) to the destination configured for session 1.
- **Loss of Connectivity Suspends Remote Mirroring:** When a remote mirroring session is configured on a source switch, the switch sends an ARP request to the configured destination approximately every 60 seconds. If the source switch fails to receive the expected ARP response from the destination for that session, transmission of mirrored traffic for the session halts. However, because the source switch continues to send ARP

requests for each configured remote session, link restoration or discovery of another path to the destination enables the source switch to resume transmitting the session's mirrored traffic after a successful ARP/ response cycle occurs. Note that if a link's connectivity is repeatedly interrupted ("link toggling"), little or no mirrored traffic may be allowed for any sessions using that link. To verify the status of any mirroring session configured on the source switch, use **show monitor**.

Troubleshooting Mirroring

Mirrored traffic does not reach configured remote destination switch or remote exit port.

- For a given mirroring session, the **mirror** command parameters configured on the source switch for source IP address, source UDP port, and destination IP address must be identical to their counterparts in the **mirror endpoint** command configured on the destination switch.
- The configured exit port must not be a member of a trunk or mesh.
- If the destination for mirrored traffic is on a different VLAN than the source, routing must be correctly configured along the path from the source to the destination.
- On the destination switch for a given mirroring session, both the port on which the mirrored traffic enters the switch and the exit port must be members of the same VLAN.
- All links on the path from the source switch to the destination switch must be active.

Caution

A mirroring exit port should be connected only to a network analyzer, IDS, or other network edge device that has no connection to other network resources. Allowing a mirroring exit port connection to a network can result in serious network performance problems, and is strongly discouraged by ProCurve Networking.

Locating a Device

If you are trying to locate a particular switch you can enter the **chassislocate** command. The blue Locator LED will light up on that switch.

Syntax: chassislocate [blink | on | off]

Locate a device by using the blue Locate LED on the front panel.

blink <1-1440>

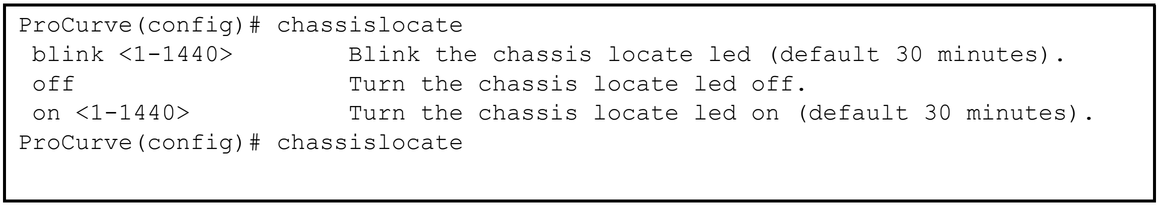
Blinks the chassis Locate LED for a selected number of minutes (default is 30 minutes).

on <1-1440>

Turns the chassis Locate LED on for a selected number of minutes (default is 30 minutes).

off

Turns the chassis Locate LED off.



```
ProCurve(config)# chassislocate
 blink <1-1440>        Blink the chassis locate led (default 30 minutes).
 off                   Turn the chassis locate led off.
 on <1-1440>           Turn the chassis locate led on (default 30 minutes).
ProCurve(config)# chassislocate
```

Figure B-41. The chassislocate command

For redundant management systems, if the active management module fails-over, the Locator LED does not remain lit.