Software Update C.07. *XX* Release Notes *for the* HP ProCurve Switch 1600M, 2400M, 2424M, 4000M, and 8000M

If you received this booklet with the purchase of an HP ProCurve Switch 1600M, 2424M, 4000M, or 8000M, then software release C.07.XX is included in your switch.

Software Updates Are Free!

Hewlett-Packard provides free software updates on the HP ProCurve website. To automatically receive email notice of new updates for *all* managed ProCurve and AdvanceStack networking products, just fill out and mail the postage-paid card attached to the TopTools CD sleeve included with your switch. Look for the CD sleeve with *Your Free Ticket to Proactive Networking* on the cover. (If you have already mailed one of these cards for another HP networking product, it is not necessary to send in the card again.)

To determine whether you have the latest software, and to access software updates on the web, go to the ProCurve website at **http://www.hp.com/go/procurve**, then click on **Support** and look for the link to use for accessing and downloading software.

Included in This Booklet

- Configuring and Monitoring Port Security—page 4
- Enhancing Security By Configuring Authorized IP Managers—page 15
- Class of Service (CoS): Managing Bandwidth More Effectively—page 22

Publication Number

5969-2305
April 1999

Applicable Product

HP ProCurve Switch 1600M (J4120A)
HP ProCurve Switch 2424M (J4093A)
HP ProCurve Switch 4000M (J4121A)
HP ProCurve Switch 8000M (J4110A)

Trademark Credits

Microsoft, Windows, Windows 95, and Microsoft Windows NT are registered trademarks of Microsoft Corporation. Internet Explorer is a trademark of Microsoft Corporation. Ethernet is a registered trademark of Xerox Corporation. Netscape is a registered trademark of Netscape Corporation.

Disclaimer

The information contained in this document is subject to change without notice.

HEWLETT-PACKARD COMPANY MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Hewlett-Packard assumes no responsibility for the use or reliability of its software on equipment that is not furnished by Hewlett-Packard.

Warranty

See the Customer Support/Warranty booklet included with the product.

A copy of the specific warranty terms applicable to your Hewlett-Packard products and replacement parts can be obtained from your HP Sales and Service Office or authorized dealer.

Hewlett-Packard Company
8000 Foothills Boulevard, m/s 5552
Roseville, California 95747-5552
http://www.hp.com/go/procurve

Contents

Configuring and Monitoring Port Security 4
Basic Operation 4
Configuring Port Security 5
Reading and Resetting Intrusion Alarms 11
Operating Notes for Port Security 14
Enhancing Security By Configuring Authorized IP Managers 15
Access Levels 15
Defining Authorized Management Stations 16
Configuring IP Authorized Managers in the Web Browser Interface . . 17
Configuring IP Authorized Managers in the Console Interface 17
Building IP Masks 19
Operating and Troubleshooting Notes 21
Class of Service (CoS): Managing Bandwidth More Effectively . . . 22
Definitions 23
Basic Operation 23
Criteria for Prioritizing Outbound Packets 24
How To Configure CoS 26
Configuring Class of Service from the Web Browser Interface 27
Configuring Class of Service from the Console 29
Using Type of Service (ToS) Criteria to Prioritize IP Traffic 33
IP Multicast (IGMP) Interaction with CoS 35
Summary of CoS Operation 36
Supporting CoS with an 802.1Q Tagged VLAN Environment 40
Operating and Troubleshooting Notes 40

Configuring and Monitoring Port Security

Using Port Security, you can configure each switch port with a unique list of the MAC addresses of devices that are authorized to access the network through that port. This enables individual ports to detect, prevent, and log attempts by unauthorized devices to communicate through the switch.

Basic Operation

The default port security setting for each port is "off". That is, any device can access a port without causing a security reaction. However, on a per-port basis, you can configure security measures to block unauthorized connections or "listening", and to send notice of security violations. Once you have configured port security, you can then monitor the network for security violations through one or more of the following:

- Alert flags that are captured by network management tools such as HP TopTools for Hubs & Switches
- Alert Log entries in the switch's web browser interface
- Event Log entries in the console interface
- Intrusion Log entries in either the switch's web browser interface or console interface

For any port, you can configure the following:

- **Authorized Addresses:** Specify up to eight devices (MAC addresses) that are allowed to send inbound traffic through the port. This feature:
  - Closes the port to inbound traffic from any unauthorized devices that are connected to the port.
  - Automatically sends notice of an attempted security violation to the switch's Intrusion Log and to the Alert Log in the switch's web browser interface.
  - Sends an SNMP trap notifying of an attempted security violation to a network management station. (For more on configuring the switch for SNMP management, see the *Management and Configuration Guide* you received with the switch.)
- **Prevent Eavesdropping:** Block outbound traffic with unknown destination addresses from exiting through the port. This prevents an unauthorized device on the port from eavesdropping on the flooded unicast traffic intended for other devices.

Note: The switch security measures block unauthorized traffic without disabling the port. This implementation enables you to apply the security configuration to ports on which hubs or other switches are connected, and to maintain security while also maintaining network access to authorized users.

Configuring Port Security

Planning

1. Plan your port security configuration and monitoring according to the following:
   a. On which ports do you want to configure intruder security?
   b. Which devices (MAC addresses) are authorized on each port?
   c. For each port, what security actions do you want? You can do one or both of the following:
      – Block intruders from transmitting to the network
      – Prevent intruders from eavesdropping on network traffic
   d. How do you want to learn of the security violation attempts the switch detects? You can use one or more of these methods:
      – Through network management (That is, do you want an SNMP trap sent to a net management station when a port detects a security violation attempt?)
      – Through the switch's web browser interface (Alert Log and Intrusion Log)
      – Through the Event Log and the Intrusion Log in the switch console interface
2. Use the web browser interface and/or the switch console to configure port security. The following table describes the parameters.

Table 1. Port Security Control Parameters

Parameter	Description
Port	Identifies the switch port to view or configure for port security.
Learn Mode	Specifies how the port will acquire its list of authorized addresses. **Continuous (the default):** Allows the port to learn addresses from inbound traffic from any device(s) to which it is connected. In this state, the port accepts as authorized any device(s) to which it is connected. Addresses learned this way appear in the switch and port address tables and age out according to the Address Age interval in the System Information configuration screen. **Static:** Enables you to specify how many devices are authorized on the port and to enter the MAC addresses of the authorized devices. If you enter fewer MAC addresses than you authorized, the port learns the remaining addresses from the inbound traffic it receives. (See "Authorized Addresses" at the end of this table.) **Note:** When you configure Learn Mode to **Static**, all devices (MAC addresses) in the port's address table are deleted (from both the port's address table and the switch's address table) and replaced by the authorized devices for this port.
Address Limit	When Learn Mode is set to Static, specifies how many authorized devices (MAC addresses) to allow. Range: 1 (the default) to 8.

— Continued on Next Page —

Parameter	Description
Eavesdrop Prevention	Specifies whether the port will block outbound traffic addressed to devices unknown to the port (that is, flooded unicast traffic). This is recommended for use on secure ports with known (static) MAC addresses, which make it unnecessary for these ports to transmit flooded unicast traffic for unknown destinations. **Disabled (the default):** Allow the port to transmit all outbound traffic it receives, regardless of whether the traffic is addressed to devices that are known to the port. **Enabled:** Allows the port to transmit only the outbound traffic addressed to devices that are known to the port. (Outbound traffic to devices unknown to the port is dropped.) Devices known to the port include all devices (MAC addresses) the port has detected and listed in its address table, and any devices configured in the Authorized Addresses table. (You can view the port's address table from the console Status and Counters menu. The Authorized Addresses table appears if the Learn Mode parameter is set to **Static**. **Note:** This feature is not recommended for applications in which a port's Learn Mode is configured to Continuous.
Action	Specifies whether an SNMP trap is sent to a network management station when Learn Mode is configured to **Static** and the port detects an unauthorized device. **None (the default):** Prevents an SNMP trap from being sent. **Send Alarm:** Causes the switch to send an SNMP trap to a network management station. For information on configuring the switch for SNMP management, see the *Management and Configuration Guide* you received with the switch.
Authorized Addresses	Appears when Learn Mode is set to Static. Enables you to enter up to eight authorized devices (MAC addresses) per port, depending on the value specified in the Address Limits field. If you enter fewer devices than you specified in the Address Limits field, the port learns the remaining addresses from the inbound traffic it receives. For example, if you specify four devices, but enter only two MAC addresses, the first two (non-specified) devices subsequently detected on the port will be added to the Authorized Address list, and all subsequent (non-specified) devices detected on the port will be handled as "unauthorized". **Caution:** If you enter fewer devices (MAC addresses) than specified in the Address Limits parameter, it is possible to unintentionally allow a device to become "authorized" that you do not want to include in your Authorized Address list. This can occur because the port, in order to fulfill the number of devices allowed by the Address Limits parameter, will automatically add devices it detects until the specified limit is reached. For this reason it is recommended that you configure the Address Limit to allow only as many devices as you plan to type in to the Authorized Addresses list.

Using the Web Browser Interface to Configure Port Security

1. Display the Port Security Screen

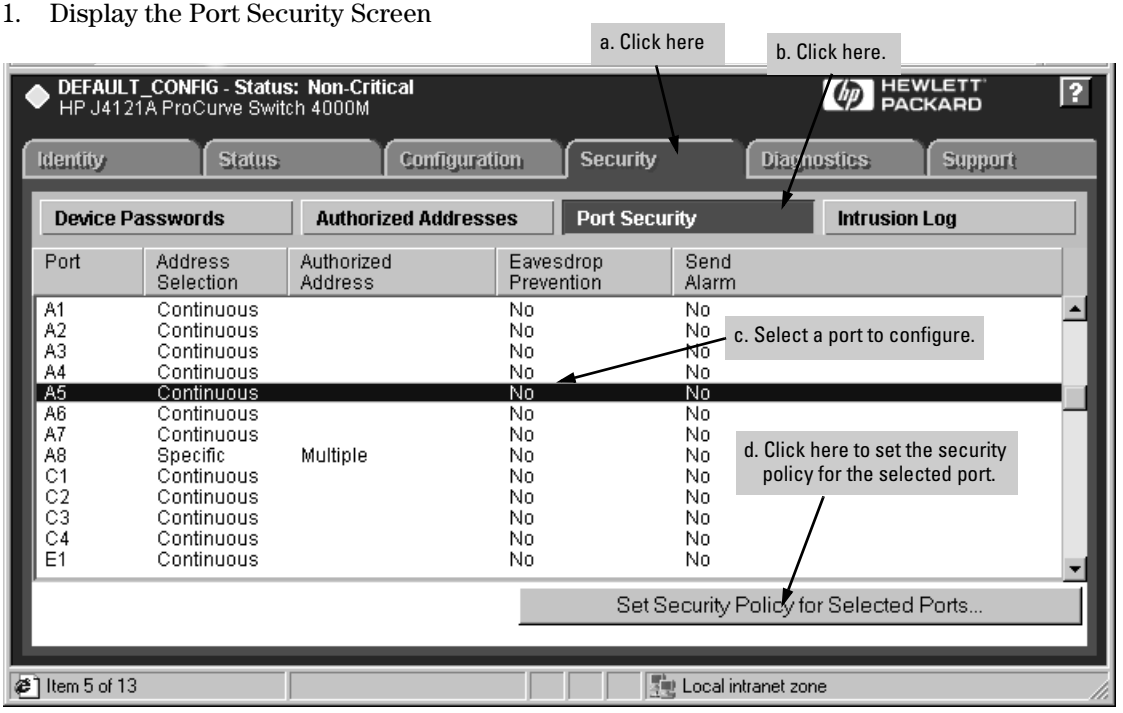

Figure 1. Example of the Port Security Overview Screen

2. Set the security policy for the selected port.

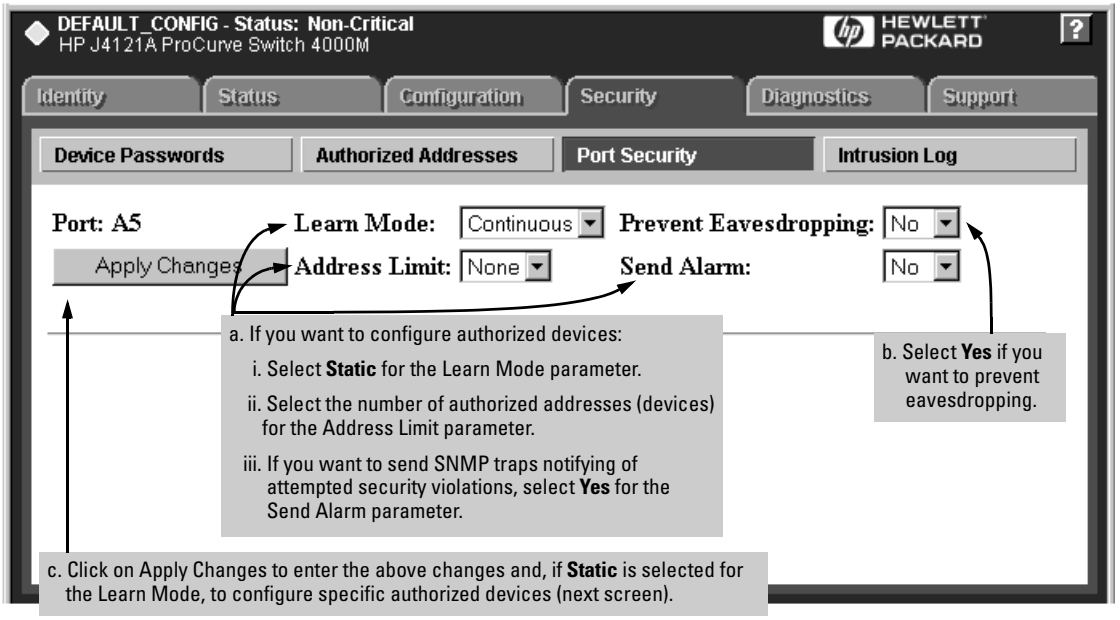

Figure 2. Example of the Default Security Configuration Screen for a Selected Port

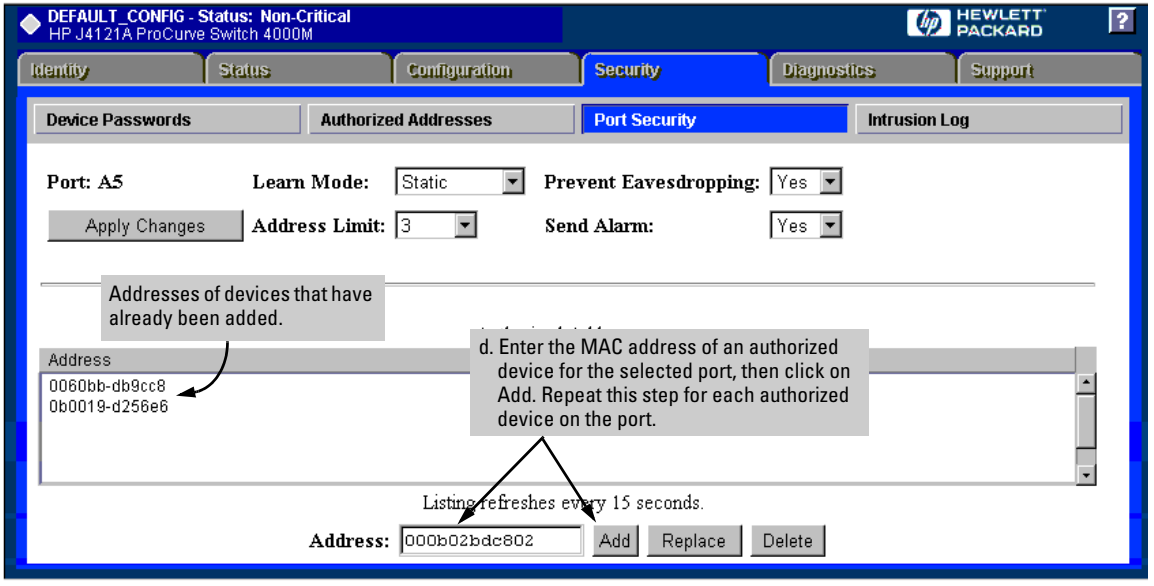

Figure 3. Example of Adding Authorized Devices

Using the Switch Console To Configure Port Security

From the Main Menu, select:

Switch Configuration . . .

Advanced Features . . .

Port Security

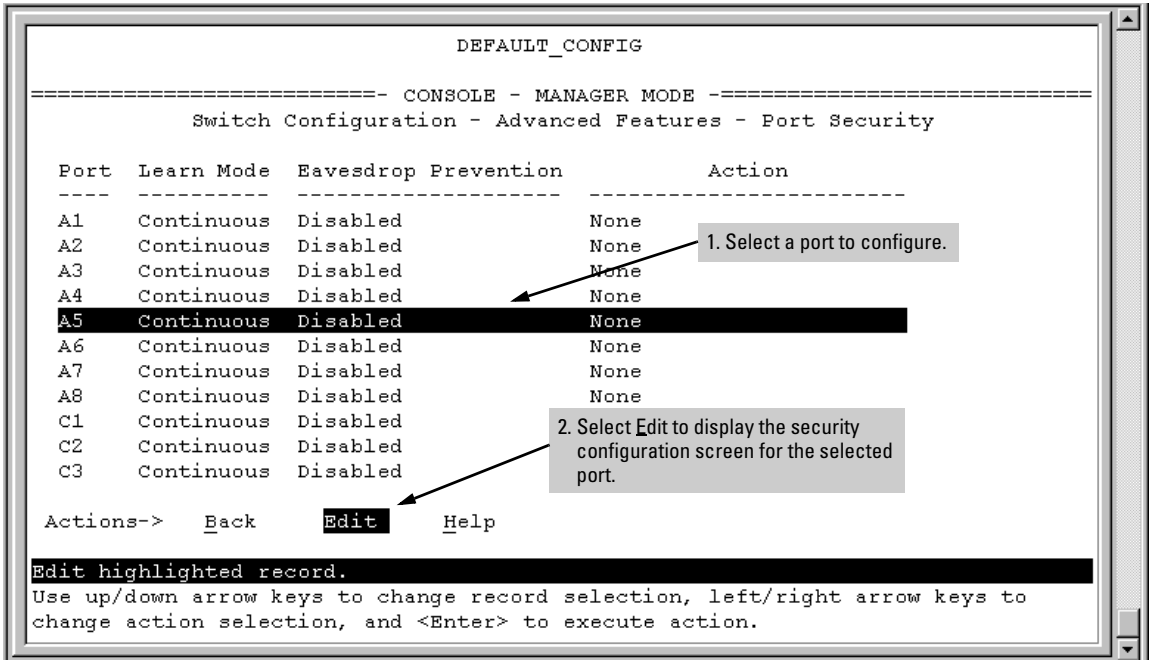

Figure 4. Example of the Default Security Configuration Screen for a Selected Port

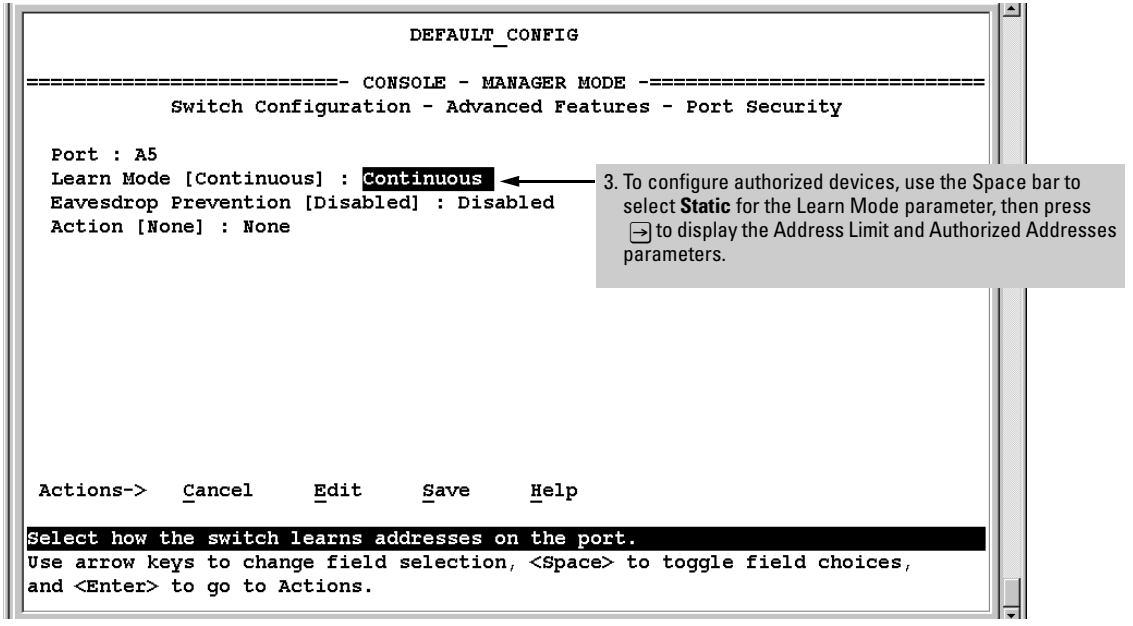

Figure 5. Example of the Default Security Configuration Screen for a Selected Port

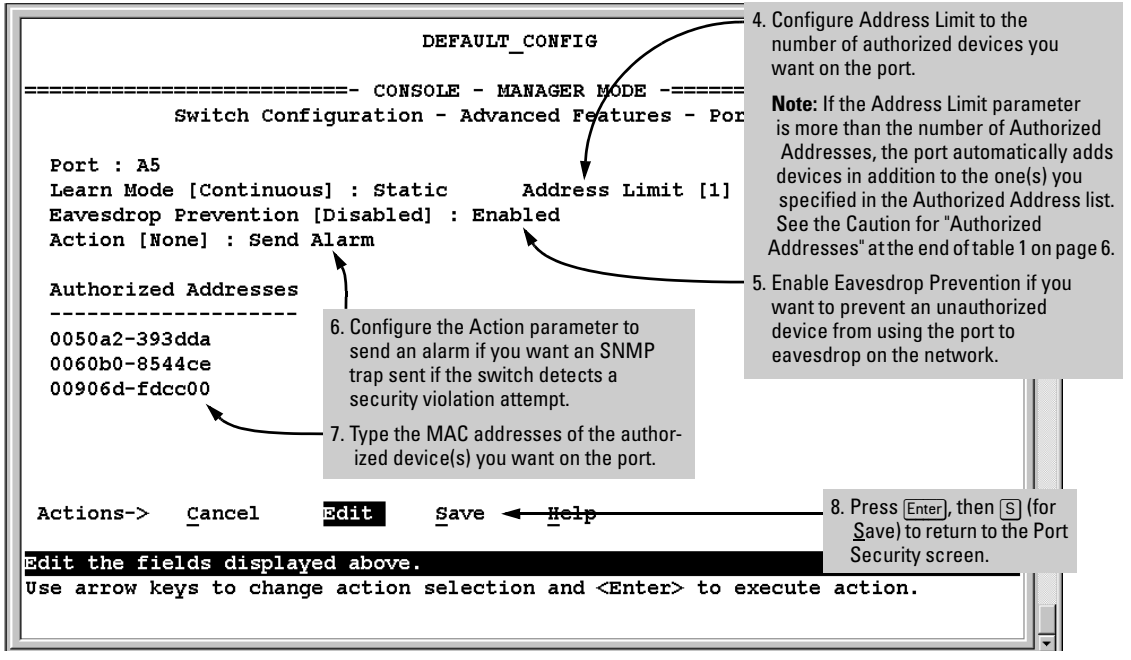

Figure 6. Example of a Modified Security Configuration Screen for a Selected Port

Reading and Resetting Intrusion Alarms

When an attempted security violation occurs on a port configured for Port Security, the port drops the packets it receives from the unauthorized device.

Notice of Security Violations

When a security violation occurs on a port configured for Port Security, the switch responds in the following ways to notify you:

- The switch sets an alert flag for that port. This flag remains until:
  - You use either the console or web browser interface to reset the flag
  - The switch is reset to its factory default
- The web browser and console interfaces notify you of the intrusion.
  - In the web browser interface:
    - The Alert Log displays a Security Violation entry, with the system date and time, and the port on which the violation occurred (figure 7, below).
    - The Intrusion Log lists the port number, the MAC address of the intruding device, and the system time and date when the intrusion occurred (figure 8 on page 12).

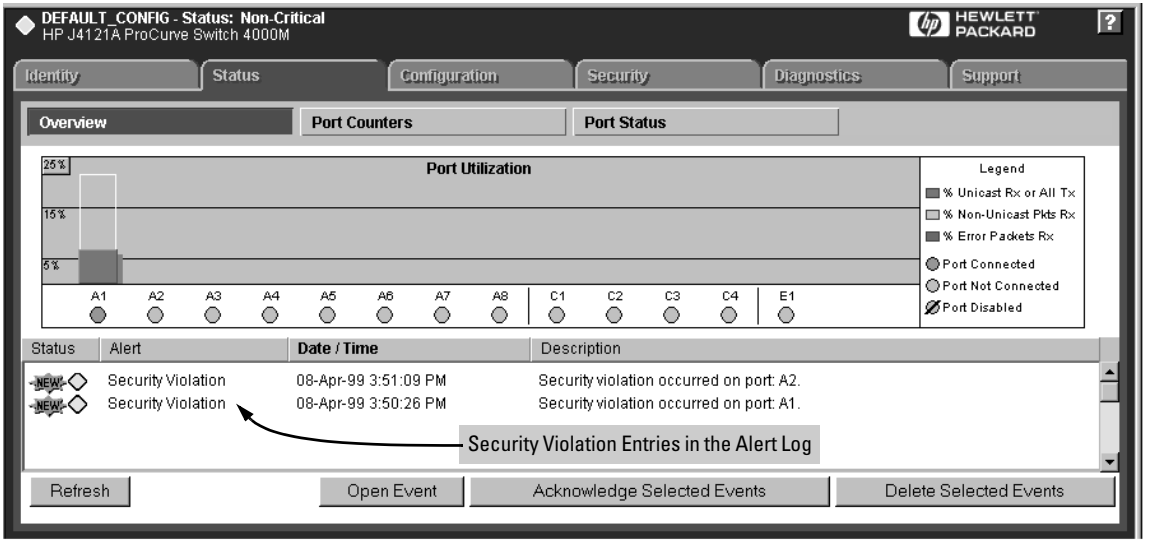

Figure 7. Example of Security Violation Entries in the Alert Log of the Switch's Web Browser Interface

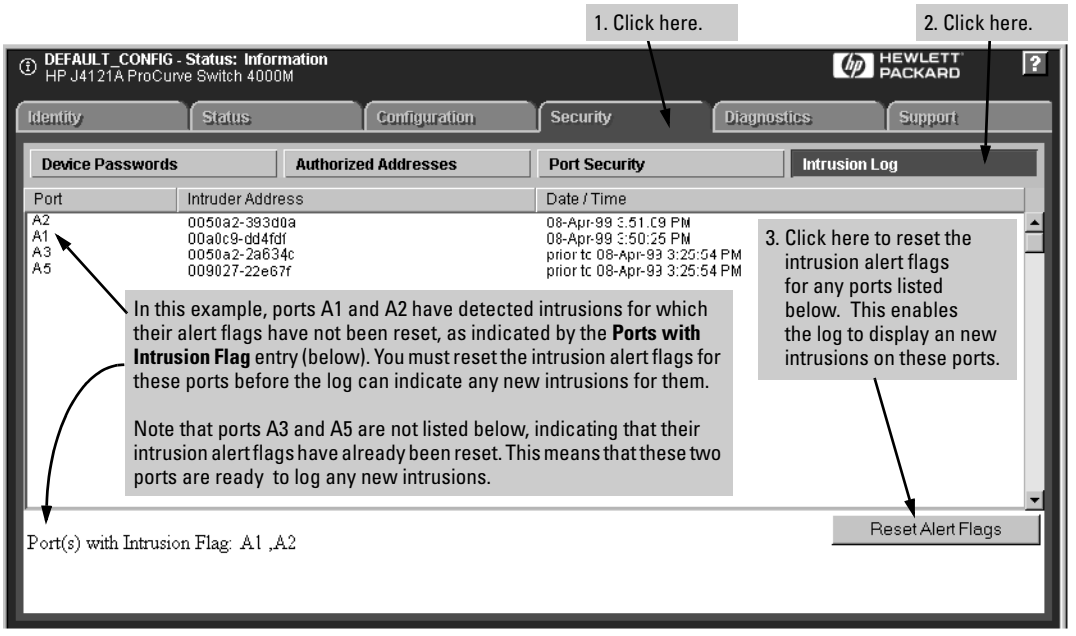

Figure 8. Example of the Intrusion Log with Intrusions Entered for Ports A1 and A2

- In the switch console:
  - The switch console Event Log, accessed from the Main Menu, displays the intrusion as an FFI (Find, Fix, and Inform) Security Violation event with the related port number (figure 9, below).

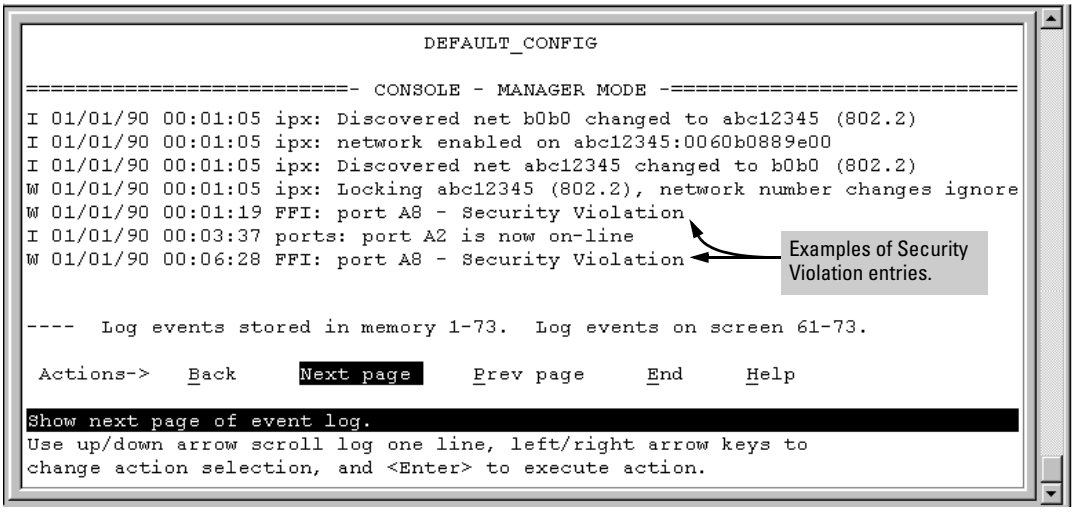

Figure 9. Example of the Switch Console Event Log with Security Violation Entries

- The Intrusion Alert column in the console's Port Status screen displays **Yes** for the port on which the violation occured (figure 10, below).

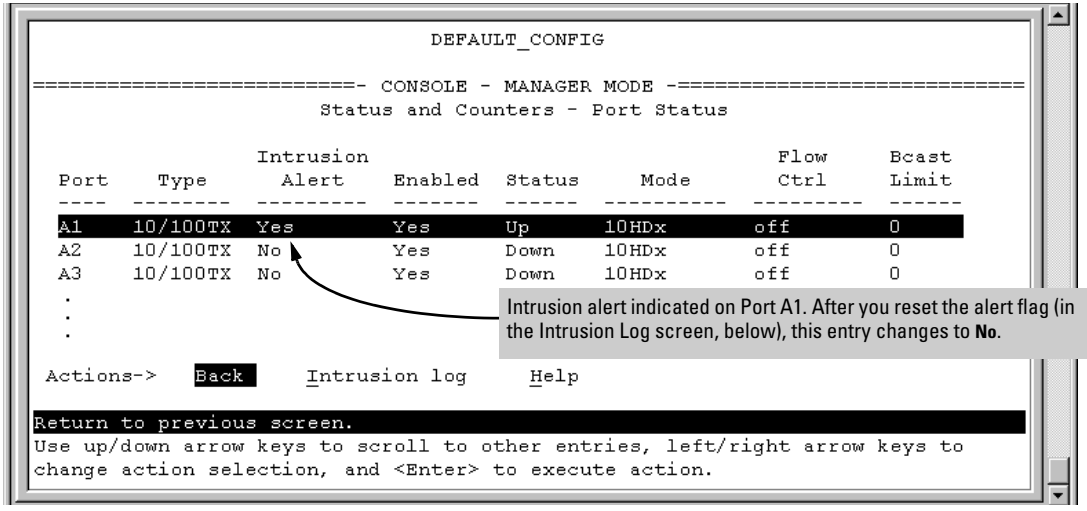

Figure 10. Example of Port Status Screen with Intrusion Alert on Port A1

- The console's Intrusion Log lists the port number, the MAC address of the intruding device, and the system time and date when the intrusion occurred (figure 11, below).

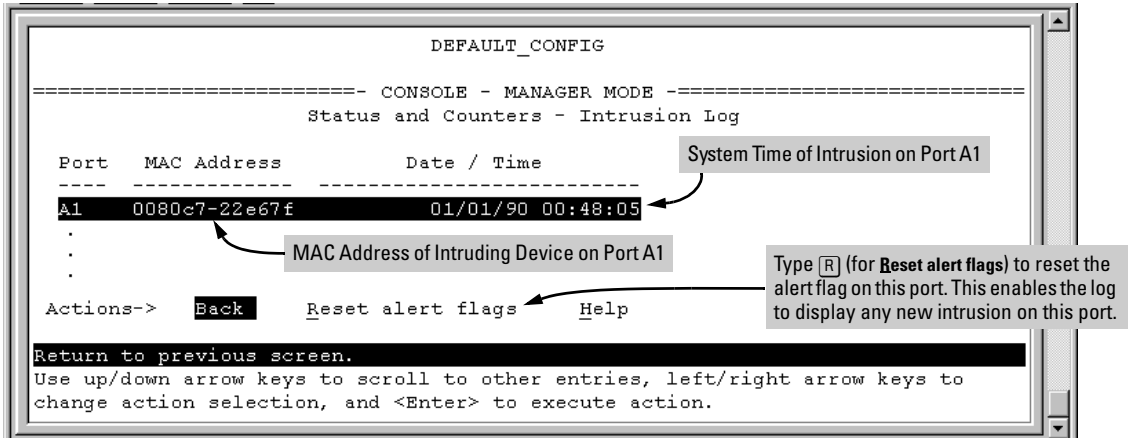

Figure 11. Example of the Intrusion Log with an Intrusion Listed for Port A1

How the Intrusion Log Operates

The Intrusion Log gives you a list of the 20 most recent security violation attempts, and appears in both the web browser interface and the switch console. The log shows the most recent intrusion at the top of the listing. You cannot delete Intrusion Log entries. Instead, if the log is filled when the switch detects a new intrusion, the oldest entry is dropped off the listing and the newest entry appears at the top of the listing.

Keeping the Intrusion Log Current by Resetting Alert Flags. When a violation occurs on a port, an alert flag is set for that port and the violation is entered in the Intrusion Log. The switch can detect and handle subsequent intrusions on that port, but will not log another intrusion on the port until you go to the Intrusion Log and use the Reset Alert Flags button to reset the port's alert flag.

Operating Notes for Port Security

Identifying the IP Address of an Intruder. The Intrusion Log lists intruders by MAC address. If you are using HP TopTools for Hubs & Switches to manage your network, you can use the TopTools inventory reports to link MAC addresses to their corresponding IP addresses. (Inventory reports are organized by device type; hubs, switches, servers, etc.)

Proxy Web Servers. If you are using the switch's web browser interface through a switch port configured for Static port security, and your browser access is through a proxy web server, then it is necessary to do the following:

- Enter your PC or workstation MAC address in the port's Authorized Addresses list.
- Enter your PC or workstation's IP address in the switch's IP Authorized Managers list. See "Enhancing Security by Configuring Authorized Managers" on page 15.)

Without both of the above configured, the switch detects only the proxy server's MAC address, and not your PC or workstation MAC address, and interprets your connection as unauthorized. For more on web proxy servers, see "Web Proxy Servers" on page 21.

Security Violations. If you reset the switch (using the Reset button, Device Reset, or Reboot Switch), the Intrusion Log will list the time of all currently logged intrusions as "prior to" the time of the reset.

Alert Flag Status for Entries Forced Off of the Intrusion Log. If the Intrusion Log is full of entries for which the alert flags have not been reset, a new intrusion will cause the oldest entry to drop off the list, but will not change the alert flag status for the port referenced in the dropped entry. This means that, even if an entry is forced off of the Intrusion Log, no new intrusions can be logged on the port referenced in that entry until you reset the alert flags.

Enhancing Security By Configuring Authorized IP Managers

This feature enables you to enhance security on the switch by using IP addresses to authorize which stations (PCs or workstations) are allowed to:

- Access the switch's web browser interface
- Telnet into the switch's console interface
- Perform TFTP transfers of configurations and software updates into the switch

---

Note

This feature does not affect SNMP access to the switch by SNMP-authorized management stations. (SNMP access is protected by community names and an independent SNMP Authorized Managers list.)

You can configure:

- Up to 10 authorized manager addresses, where each address applies to either a single management station or a group of stations
- Either a Manager or Operator access level

Note

This feature does not protect access to the switch through a modem or direct Console (RS-232) port connection. Also, if the IP address assigned to an authorized management station is configured in another station, the other station can gain management access to the switch even though a duplicate IP address condition exists. For these reasons, you should enhance your network's security by keeping physical access to the switch restricted to authorized personnel, using the password features built into the switch, and preventing unauthorized access to data on your management stations.

Access Levels

For each authorized manager address, you can configure either one of these access levels:

- **Manager:** Enables full access to all web browser and console interface screens for viewing, configuration, and all other operations available in these interfaces.

- **Operator:** Allows view-only access from the web browser and console interfaces. (This is the same access that is allowed by the switch's operator-level password feature.)

Defining Authorized Management Stations

- **Authorizing Single Stations:** Enable only one station per Authorized Manager IP parameter to access the switch (the default). To use this method, just enter the IP address of an authorized management station in the Authorized Manager IP parameter, and leave the IP Mask set to **255.255.255.255**. This is the easiest way to use the Authorized Managers feature. (For more on this topic, see "Configuring One Station Per Authorized Manager IP Entry" on page 19.)

- **Authorizing Multiple Stations:** Using one Authorized Manager IP parameter, enable a defined group of stations to access the switch. This is useful if you want to authorize several stations for either manager- or operator-level access to the switch. All stations in a group defined by one Authorized Manager IP parameter and its associated IP mask will have the same access level—Manager or Operator. (For more on this topic, see "Configuring Multiple Stations Per Authorized Manager IP Entry" on page 19.)

To configure the switch for authorized manager access, enter the appropriate *Authorized Manager IP* parameter, specify an *IP Mask*, and select either **Manager** or **Operator** for the *Access Level*. The IP Mask determines how the Authorized Manager IP parameter is used to define authorized IP addresses for management station access.

Overview of IP Mask Operation. The default IP Mask is 255.255.255.255 and allows switch access only to a station having an IP address that is identical to the Authorized Manager IP parameter. ("255" in an octet of the mask means that only the exact value in the corresponding octet of the Authorized Manager IP parameter is allowed in the IP address of an authorized management station.) However, you can alter the mask and the Authorized Manager IP parameter to specify ranges of authorized IP addresses. For example, a mask of **255.255.255.*0*** and any value for the Authorized Manager IP parameter allows a range of 0 through 255 in the 4th octet of the authorized IP address, which enables a block of up to 256 IP addresses for IP management access. A mask of **255.255.255.25*2*** uses the 4th octet of a given Authorized Manager IP address to authorize four IP addresses for management station access. The details on how to use IP masks are provided under "Building IP Masks" on page 19.

Note

The IP Mask is a method for recognizing whether a given IP address is authorized for management access to the switch. This mask serves a different purpose than IP subnet masks and is applied in a different manner.

Configuring IP Authorized Managers in the Web Browser Interface

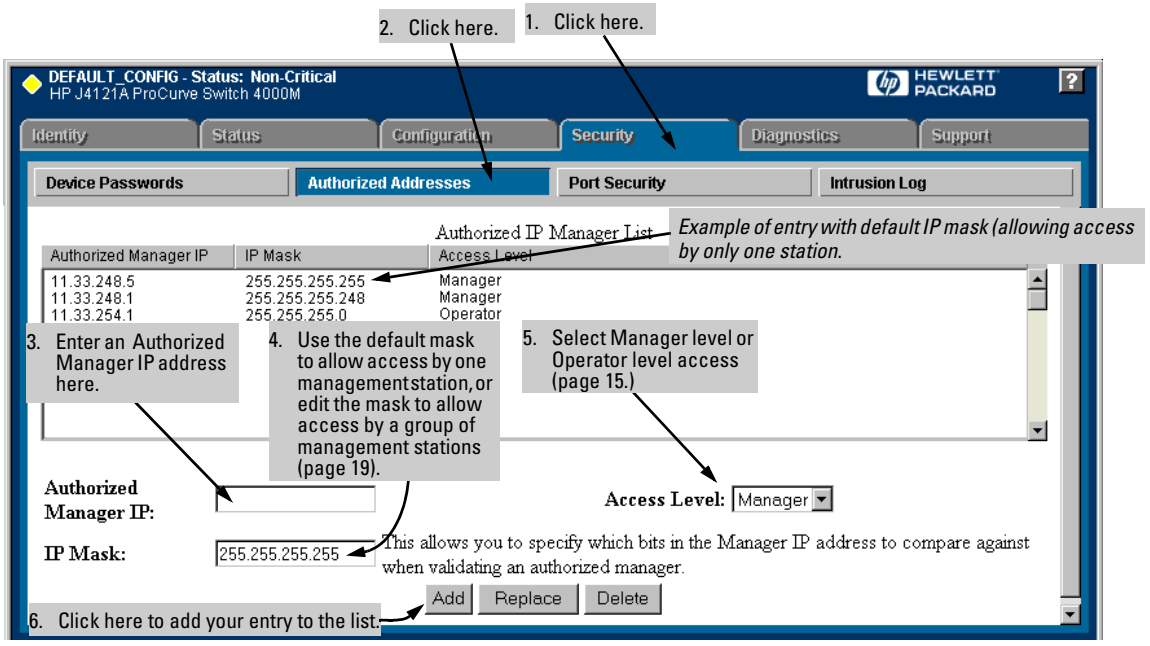

Figure 12. Example of an Authorized IP Manager List with Manager and Operator Assignments

Configuring IP Authorized Managers in the Console Interface

From the console Main Menu, select:

Switch Management Access Configuration (IP, SNMP, Console) . . .
IP Authorized Managers

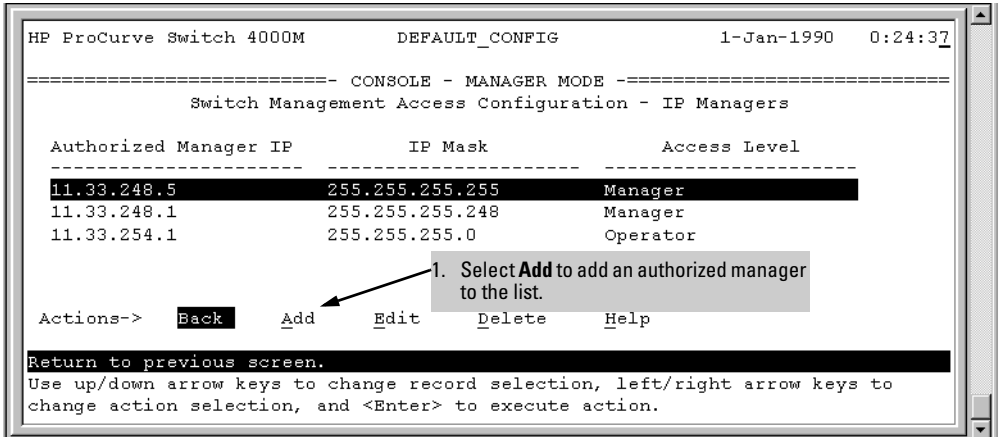

Figure 13. Example of How To Add an Authorized Manager Entry

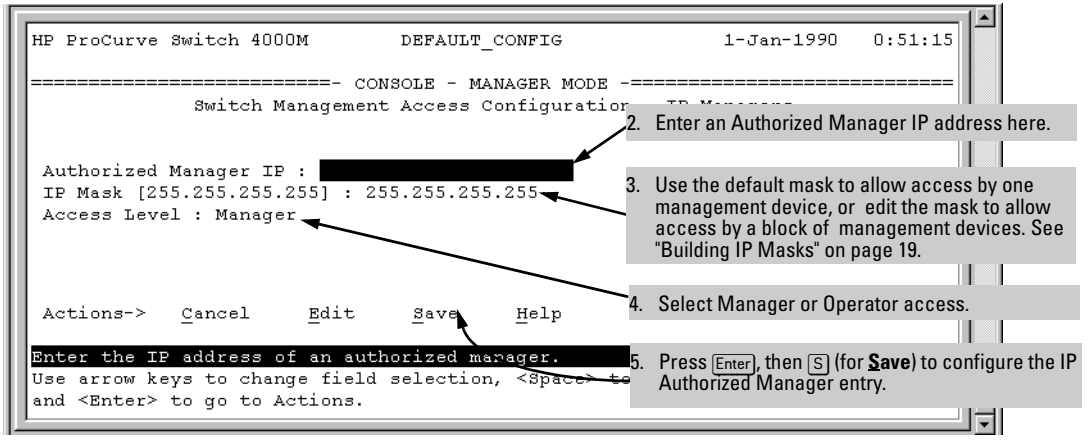

Figure 14. Example of How To Add an Authorized Manager Entry (Continued)

Editing or Deleting an Authorized Manager Entry. Go to the IP Managers List screen (figure 13), highlight the desired entry, and press E (for **Edit**) or D (for **Delete**).

Building IP Masks

The IP Mask parameter controls how the switch uses an Authorized Manager IP value to recognize the IP addresses of authorized manager stations on your network.

Configuring One Station Per Authorized Manager IP Entry

This is the easiest way to apply a mask. If you have ten or fewer management and/or operator stations, you can configure them quickly by simply adding the address of each to the Authorized Manager IP list with **255.255.255.255** for the corresponding mask. For example, as shown in figure 12 on page 17, if you configure an IP address of **11.33.248.5** with an IP mask of **255.255.255.255**, only a station having an IP address of 11.33.248.5 has management access to the switch.

Table 2. Analysis of IP Mask for Single-Station Entries

	1st Octet	2nd Octet	3rd Octet	4th Octet	Manager-Level or Operator-Level Device Access
IP Mask	255	255	255	255	The "255" in each octet of the mask specifies that only the exact value in that octet of the corresponding IP address is allowed. This mask allows management access only to a station having an IP address of 11.33.248.5.
Authorized Manager IP	11	33	248	5	

Configuring Multiple Stations Per Authorized Manager IP Entry

The mask determines whether the IP address of a station on the network meets the criteria you specify. That is, for a given Authorized Manager entry, the switch applies the IP mask to the IP address you specify to determine a range of authorized IP addresses for management access. As described above, that range can be as small as one IP address (if **255** is set for all octets in the mask), or can include multiple IP addresses (if one or more octets in the mask are set to less than **255**). If a bit in an octet of the mask is “on” (set to 1), then the corresponding bit in the IP address of a potentially authorized station must match the same bit in the IP address you entered in the Authorized Manager IP list. Conversely, if a bit in an octet of the mask is “off” (set to 0), then the corresponding bit in the IP address of a potentially authorized station on the network does not have to match its counterpart in the IP address you entered in the Authorized Manager IP list. Thus, in the example shown above, a “255” in an IP Mask octet (*all* bits in the octet are “on”) means only one value is allowed for that octet—the value you specify in the corresponding octet of the Authorzed Manager IP list. A “0” (all bits in the octet are “off”) means that any value from 0 to 255 is allowed in the corresponding octet in the IP address of an authorized station. You can also specify a series of values that are a subset of the 0-255 range by using a value that is greater than 0, but less than 255.

Table 3. Analysis of IP Mask for Multiple-Station Entries

	1st Octet	2nd Octet	3rd Octet	4th Octet	Manager-Level or Operator-Level Device Access
IP Mask	255	255	255	0	The "255" in in the first three octets of the mask specify that only the exact value in the octet of the corresponding IP address is allowed. However, the zero (0) in the 4th octet of the mask allows any value between 0 and 255 in that octet of the corresponding IP address. This mask allows switch access to any device having an IP address of 11.33.248.*xxx*, where *xxx* is any value from 0 to 255.
Authorized Manager IP	11	33	248	5	
IP Mask	255	255	255	249	In this example (figure 15, below), the IP mask allows a group of up to 4 management stations to access the switch. This is useful if the only devices in the IP address group allowed by the mask are management stations. The "249" in the 4th octet means that bits 0 and 3 - 7 of the 4th octet are fixed. Conversely, bits 1 and 2 of the 4th octet are variable. Any value that matches the authorized IP address settings for the fixed bits is allowed for the purposes of IP management station access to the switch. Thus, any management station having an IP address of 11.33.248.1, 3, 5, or 7 can access the switch.
Authorized IP Address	11	33	248	5	

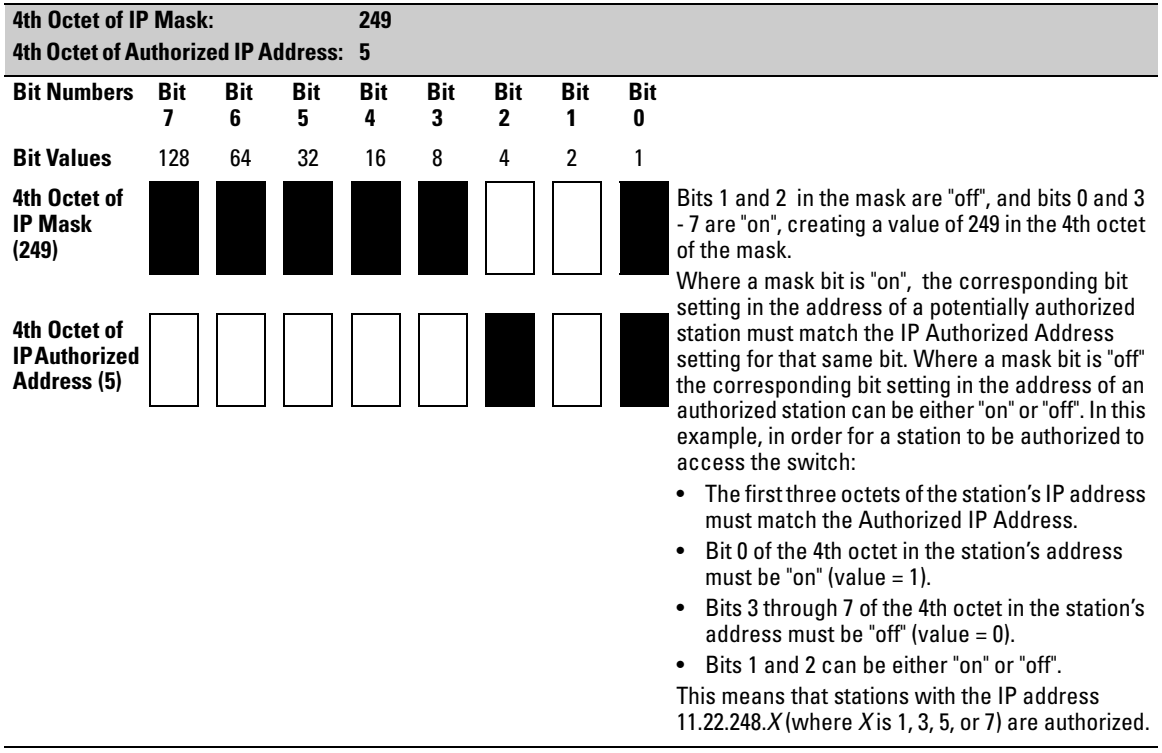

Figure 15. Example of How the Bitmap in the IP Mask Defines Authorized Manager Addresses

Additional Examples of Authorized Manager Entries for Multiple Stations

	Entries for Authorized Manager List				Results
IP Mask	255	255	0	255	This combination specifies an authorized IP address of 10.33.*xxx*.1. It could be applied, for example, to a subnetted network where each subnet is defined by the third octet and includes a management station defined by the value of "1" in the fourth octet of the station's IP address.
Authorized Manager IP	10	33	248	1	
IP Mask	255	238	255	250	Allows 230, 231, 246, and 247 in the 2nd octet, and 194, 195, 198, 199 in the 4th octet.
Authorized Manager IP	10	247	100	195	

Operating and Troubleshooting Notes

- **Network Security Precautions:** You can enhance your network's security by keeping physical access to the switch restricted to authorized personnel, using the password features built into the switch, and preventing unauthorized access to data on your management stations.
- **Modem and Direct Console Access:** Configuring authorized IP managers does not protect against access to the switch through a modem or direct Console (RS-232) port connection.
- **Duplicate IP Addresses:** If the IP address configured in an authorized management station is also configured in another station, the other station can gain management access to the switch even though a duplicate IP address condition exists.
- **Web Proxy Servers:** If you use the web browser interface to access the switch from an authorized IP manager station, it is recommended that you avoid the use of a web proxy server in the path between the station and the switch. This is because switch access through a web proxy server requires that you first add the web proxy server to the Authorized Manager IP list. This reduces security by opening switch access to anyone who uses the web proxy server. The following two options outline how to eliminate a web proxy server from the path between a station and the switch:
  - Even if you need proxy server access enabled in order to use other applications, you can still eliminate proxy service for web access to the switch. To do so, add the IP address or DNS name of the switch to the non-proxy, or "Exceptions" list in the web browser interface you are using on the authorized station.
  - If you don't need proxy server access at all on the authorized station, then just disable the proxy server feature in the station's web browser interface.

  For more information, see the online Help for the web browser you are using.

Class of Service (CoS): Managing Bandwidth More Effectively

As the term suggests, *network policy* refers to the network-wide controls you can implement to ensure uniform and efficient traffic handling throughout your network. One goal of network policy is to keep the most important traffic moving at an acceptable speed, regardless of current bandwidth usage. While adding bandwidth is always a good idea, it is not always feasible and does not completely eliminate the potential for network congestion. There will always be points in the network where multiple traffic streams merge or where network links will change speed and capacity. The impact and number of these congestion points will increase over time as more applications and devices are added to the network. When (not *if*) network congestion occurs, it is important to move traffic on the basis of relative importance. However, without *Class of Service* (CoS) prioritization, less important traffic can consume network bandwidth and slow down or halt the delivery of more important traffic. That is, without CoS, most traffic received by the switch is forwarded with the same priority it had upon entering the switch. In many cases, such traffic is "normal" priority and competes for bandwidth with all other normal-priority traffic, regardless of its relative importance to your organization's mission. This section gives an overview of CoS operation and benefits, and describes how to configure CoS in the console interface.

Class of Service is a general term for classifying and prioritizing traffic throughout a network. That is, CoS enables you to establish an end-to-end traffic priority policy to improve control and throughput of important data. You can manage available bandwidth so that the most important traffic goes first. You can use the console and web browser interface to configure CoS on individual switches having the C.07. *XX* software release. You can also configure CoS for these same switches on a network policy basis (using release N.01.03 of HP TopTools for Hubs & Switches network management software—available Summer, 1999).

CoS is implemented in the form of rules or policies that are configured on the switch. While you can use CoS to prioritize only the outbound traffic moving through the switch, you derive the maximum benefit by using CoS in an 802.1Q VLAN environment (with 802.1p priority tags), where CoS can set priorities that are supported by downstream devices. By management through prioritizing, CoS supports growth of traffic on the network while optimizing the use of existing resources—and delaying the need for further investments in equipment and services. That is, CoS enables you to:

- Specify which traffic has higher or lower priority, regardless of current network bandwidth or the relative priority setting of the traffic when it is received on the switch.
- Change (upgrade or downgrade) the priority of outbound traffic.
- Override "illegal" packet priorities set by upstream devices or applications that use 802.1Q VLAN tagging with 802.1p priority tags.
- Avoid or delay the need to add higher-cost NICs (network interface cards) to implement prioritizing. (Instead, control priority through network policy.)

Definitions

Term	Use in This Document
downstream device	A device linked directly or indirectly to an outbound switch port. That is, the switch sends traffic to downstream devices.
inbound port	Any port on the switch through which traffic enters the switch.
outbound port	Any port on the switch through which traffic leaves the switch.
outbound port queue	For any port, a buffer that holds outbound traffic until it can leave the switch through that port. There is a "high priority" queue and a "normal priority" queue for each port in the switch. Traffic in a port's high priority queue leaves the switch before any traffic in the port's normal priority queue.
precedence bits	The upper three bits in the Type of Service (ToS) field of an IP packet.
upstream device	A device linked directly or indirectly to an inbound switch port. That is, the switch receives traffic from upstream devices.
802.1p priority	A traffic priority setting carried only in packets in 802.1Q tagged VLANs. This setting can be from 0 - 7.
802.1Q tagged VLAN	A virtual LAN (VLAN) that complies with the 802.1Q standard and is configured as "tagged". (For more on VLANs, see the *Management and Configuration Guide* you received with your HP ProCurve switch.)

Basic Operation

CoS settings operate on two levels:

- **Controlling the priority of outbound packets:** Each switch port has two outbound traffic queues; "normal" priority and "high" priority. (High-priority packets leave the switch port first. Normal-priority packets leave the switch port after the port's high-priority queue is emptied.) With no CoS control, all traffic (except IGMP traffic configured for high priority) goes through the "normal" outbound port queues. However, with a CoS configuration, you can determine the outbound priority queue to which a packet is sent. (In an 802.1Q tagged VLAN environment, if CoS is *not* configured on the switch, but *is* configured on an upstream device, high priority traffic received by the switch is forwarded through high priority queues.)

- **Configuring the 802.1p priority of outbound packets in a tagged VLAN environment for use by downstream devices:** If an outbound packet is in an 802.1Q tagged VLAN environment (that is, if the packet is assigned to a tagged VLAN on the outbound port), then the packet carries an 802.1p priority setting that was configured in the switch. This priority setting can range from 0 to 7, and can be used by downstream devices having up to eight queues. Thus, while packets within the switch move only at high or normal priority, they still can carry the 802.1p priority that can be used by downstream devices having more than two priority levels. Also, if the packet enters the switch with an 802.1p priority setting, CoS can override this setting if configured to do so.

  Note: If you are not using multiple tagged VLANs in your network, you can still use the tagged VLAN feature by configuring the default VLAN as a tagged VLAN.

You can configure a CoS priority of 0 through 7 for an outbound packet. When the packet is then sent to a port, the CoS priority determines which outbound queue the packet uses:

CoS Setting	Outbound Port Queue	Operation
0 — 3	normal priority	Packets in this queue leave the port after the high-priority queue is emptied.
4 — 7	high priority	Packets in this queue leave the port first.

If a packet is not in an 802.1Q tagged VLAN environment, the above settings control only to which outbound queue the packet goes, and no 802.1p priority is added to the packet. However, if the packet is in an 802.1Q tagged VLAN environment, then the above setting is also added to the packet as an 802.1p priority that can be used by downstream devices and applications.

Table 4. Mapping Priority Settings to Device Queues

Priority Setting in the Switch	Outbound Port Queues in the Switch	802.1p Priority Setting Added to Tagged VLAN Packet Leaving the Switch	Queue Assignment in Downstream Devices With:		
			8 Queues	4 Queues	2 Queues
1	Normal	1 (low priority)	Queue 1	Queue 1	Queue 1
2	Normal	2	Queue 2		
0	Normal	0 (normal priority)	Queue 3	Queue 2	
3	Normal	3	Queue 4		
4	High	4	Queue 5	Queue 3	Queue 2
5	High	5	Queue 6		
6	High	6	Queue 7	Queue 4	
7	High	7 (high priority)	Queue 8		

Criteria for Prioritizing Outbound Packets

You can configure CoS prioritization on the basis of five packet criteria.

1. Device Priority (destination or source IP address)
2. IP Type of Service (ToS) field
3. Protocol Priority (IP, IPX, ARP, DEC LAT, AppleTalk, SNA, and NetBeui)
4. VLAN Priority
5. Incoming 802.1p Priority (present in tagged VLAN environments)

If more than one criteria is present in a packet, the switch applies a precedence scheme to the criteria and then uses only the CoS configuration for the packet criteria that has the highest precedence. For example, if CoS assigns high priority to “red” VLAN packets, but normal priority to IP packets, since Protocol Priority has precedence over VLAN priority, IP packets on the “red” VLAN will be set to normal priority. See Table 5, “Priority Criteria and Precedence,” on page 25 for more information.

Table 5. Priority Criteria and Precedence

Precedence	Criteria	Overview
1	**Device Priority (IP Address)**	You can specify a priority for any outbound packet having a particular destination or source IP address. CoS allows up to 30 IP addresses. If an outbound packet has an IP address as the destination, it takes precedence over another outbound packet that has the same IP address as a source. (This can occur, for example, on an outbound port in a switch mesh environment.) Default state: No IP address prioritization. If a packet does not meet the criteria for device priority, then precedence defaults to IP Type of Service (ToS) criteria, below.
2	**IP Type-of-Service (ToS)**	Applies only to IP packets. The ToS field in an IP packet is configured by an upstream device or application before the incoming packet enters the switch, and is not altered by the switch. CoS reads the packet's Type of Service (ToS) field and prioritizes the packet (if specified in the CoS configuration) for outbound transmission. For more on this topic, see "Using Type of Service (ToS) Criteria To Prioritize IP Traffic" on page 33. Default state: **Disabled**. If a packet does not meet the criteria for ToS priority, then precedence defaults to Protocol criteria, below.
3	**Protocol Priority**	CoS can prioritize outbound packets for one or more of these network protocols: IP, IPX, ARP, DEC LAT, AppleTalk, SNA, and NetBeui. Default state: **No override** for any protocol. If a packet does not meet the criteria for Protocol priority, then precedence defaults to VLAN criteria, below.
4	**VLAN Priority**	Enables packet priority based on the name of the VLAN in which the packet exists. For example, if the default VLAN (**DEFAULT_VLAN**) and the "Blue" VLAN are both assigned to a port, and Blue VLAN traffic is more important, you can configure CoS to give Blue VLAN traffic a higher priority than default VLAN traffic. (Priority is applied on the outbound port.) Default state: **No override**. If a packet does not meet the criteria for VLAN priority, then precedence defaults to Incoming 802.1p criteria, below.
5	**Incoming 802.1p Priority**	Where a packet enters the switch on a tagged VLAN, if CoS is not configured to apply to the packet's priority setting, the switch uses the packet's existing 802.1p priority (assigned by an upstream device or application) to determine which outbound port queue to use. If the packet leaves the switch on a tagged VLAN, then there is no change to its 802.1p priority setting. If the packet leaves the switch on an untagged VLAN, the 802.1p priority is dropped.

Entering (Inbound) 802.1p Priority	Outbound Port Queue	Exiting (Outbound) 802.1p Priority
0 - 3	Normal	0 - 3
4 - 7	High	4 - 7

If a packet does not meet the criteria for Incoming 802.1p priority, then the packet is sent to the "normal" outbound queue of the appropriate port. If the packet did not enter the switch on a tagged VLAN, but exits from the switch on a tagged VLAN, then a tagged VLAN field, including an 802.1p priority of 0 (normal), is added to the packet.

No Override. By default, the IP ToS, Protocol, and VLAN ID criteria automatically list each of their options with **No override** for priority. This means that if you do not configure a priority for a specific option, CoS does not prioritize packets to which that option applies. For example, if you do not specify a priority for the IP protocol, then the IP protocol will not be a criteria for setting a CoS priority. In this case, the packets will be handled as described above.

How To Configure CoS

You can use CoS regardless of whether your network has tagged VLANs. As described earlier (under "Basic Operation" on page 23):

- Using CoS in a tagged VLAN environment controls both of the following:
  - **Outbound port queue:** To which queue (high or normal) a packet will be sent
  - **Outbound 802.1p priority:** Enters a new 802.1p priority setting in an outbound packet or retains the packet's existing 802.1p setting. This enables the packet to carry an 802.1p priority to the next downstream device.
- Using CoS without a tagged VLAN environment affects only the outbound port queue to which a packet is sent. (That is, it prioritizes traffic flow within the switch.) However, without a tagged VLAN environment, an outbound packet cannot carry an 802.1p priority setting to a downstream device.

To configure CoS, use this procedure:

1. Determine the CoS policy you want to implement. This includes analyzing the types of traffic flowing through your network and identifying one or more traffic types to prioritize. In order of precedence, these are:
   a. Device Priority—destination or source IP address (Note that destination has precedence over source. See Table 5, "Priority Criteria and Precedence," on page 25.)
   b. IP Type of Service
   c. Protocol Priority
   d. VLAN Priority (requires at least one tagged VLAN on the network)
   e. Incoming 802.1p Priority (requires at least one tagged VLAN on the network)

   For more on how CoS operates with the above traffic types, see Table 5, "Priority Criteria and Precedence," on page 25.)
2. If you want 802.1p priority settings to be included in outbound packets, ensure that tagged VLANs are configured on the appropriate links. (See "Supporting CoS with an 802.1Q Tagged VLAN Environment" on page 40.)
3. Determine the actual CoS configuration changes you will need to make on each CoS-capable device in your network in order to implement the desired policy.

4. Configure the desired CoS priorities on the CoS-capable devices in the network. For HP devices, HP recommends that you use TopTools for Hubs & Switches (version N.01.03 or later) to help ensure that your CoS policy is implemented consistently across the network. Otherwise, use the web browser interface or the switch console interface for each device to configure CoS.

   Note: If you use TopTools for Hubs & Switches to configure CoS policy in a network, it overrides any CoS settings configured through the console or the web browser interface in any individual HP switch.

The remainder of this section describes the general process for using the web browser interface and the console interface to configure CoS.

Configuring Class of Service from the Web Browser Interface

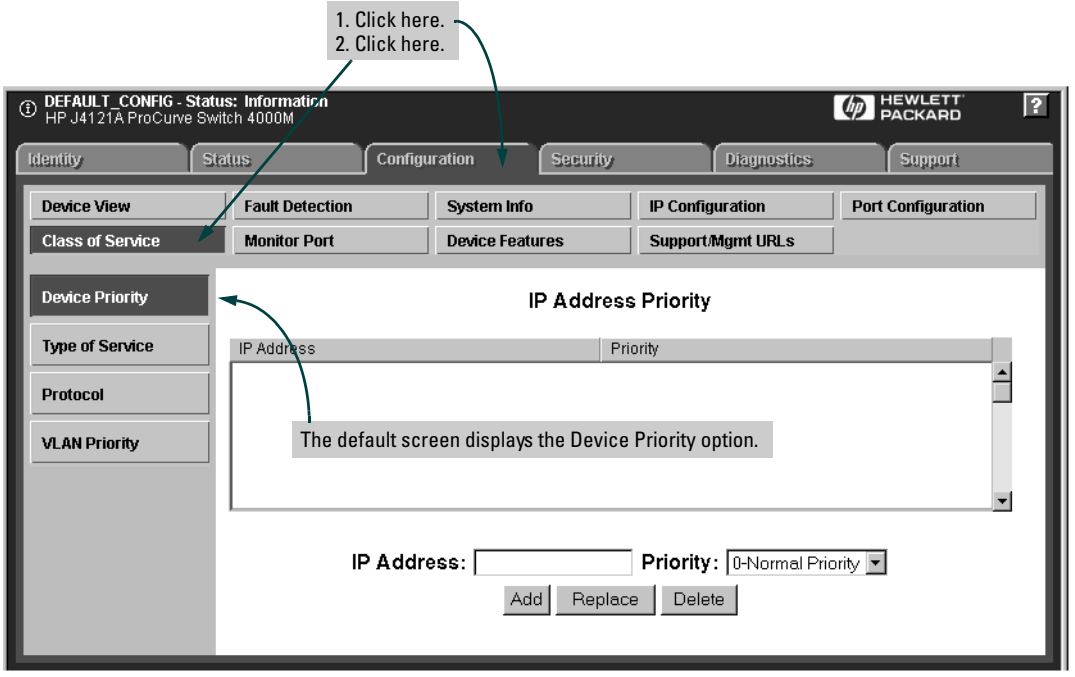

Figure 16. The Default Class of Service Configuration Screen

Use Table 6, “Steps for Using the Web Browser Interface To Configure CoS Priority” (next page) to guide you in configuring your CoS criteria.

Note: If you select “Differentiated Services” in the Type of Service option, use Telnet (to the console interface) to change the priority for a given IP ToS value.

Table 6. Steps for Using the Web Browser Interface To Configure CoS Priority

CoS Options	Priority Configuration Steps
Device Priority	Click on the **Device Priority** button, then: To add an IP address: 1. Type the address in the **IP Address** field. 2. Select the desired priority level from the **Priority** pull-down menu. 3. Click on the **Add** button. To change a configured priority for a device: 1. Type the device's IP address in the IP Address field. 2. Highlight a replacement priority level in the **Priority** pull-down menu. 3. Click on the **Replace** button. To delete a device from the Device Priority list: 1. Click on the device's IP address in the **IP Address Priority** field. 2. Click on the **Delete** button.
Type of Service	Click on the **Type of Service** button. Then: 1. Use the pull-down menu to select either IP Precedence or Differentiated Services. 2. Click on the **Apply Changes** button. If you selected Differentiated Services, you will then need to go to the Device View screen (under the Configuration tab) and Telnet to the switch console interface to change the priority for a given IP ToS value. For more on Type of Service, see "Using Type of Service (ToS) Criteria to Prioritize IP Traffic" on page 33.
Protocol	Click on the **Protocol** button. Then: 1. Click on the Priority pull-down menu for the desired protocol and select a priority level. 2. Click on the **Apply Changes** button.
VLAN Priority	Click on the VLAN Priority button. Then: **Note:** This feature configures the priority on existing VLANs (including the default VLAN). To configure new VLANs, go to the Device View screen (under the Configuration tab) and Telnet to the switch console interface. 1. Click on (highlight) the VLAN for which you want to configure a priority. 2. In the Priority pull-down menu, select the priority level you want. 3. Click on **Modify VLAN** priority.

Configuring Class of Service from the Console

CoS uses dynamic reconfiguration to configure your CoS choices. This means that it is not necessary to reboot the switch after configuring CoS.

To access the CoS console screens, begin at the Main Menu and select the following:

Switch Configuration . . .

Advanced Features . . .

Class of Service (CoS) Menu . . .

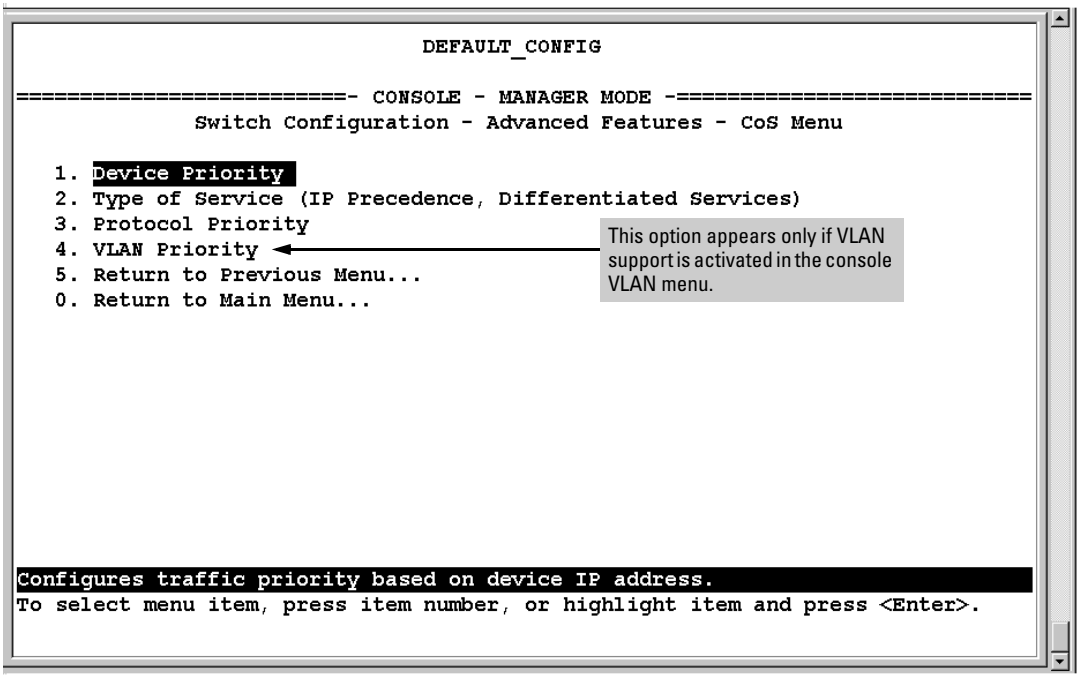

Figure 17. The Class of Service Menu

Select the priority option you want to configure for CoS. The following screens show the options with notes on how to configure them.

The CoS Device Priority Screen

CoS uses the criteria you specify per IP address (up to 30) to determine traffic prioritization. Device Priority has higher precedence than any other CoS prioritization criteria. Thus, if traffic from or to the listed devices also carries other CoS criteria, those other criteria will be ignored due to the existence of the Device Priority criteria. (For precedence information, see table 5, “Priority Criteria and Precedence”, on page 25.)

To display the Device Priority screen, select **Device Priority** in the CoS Menu screen (page 29).

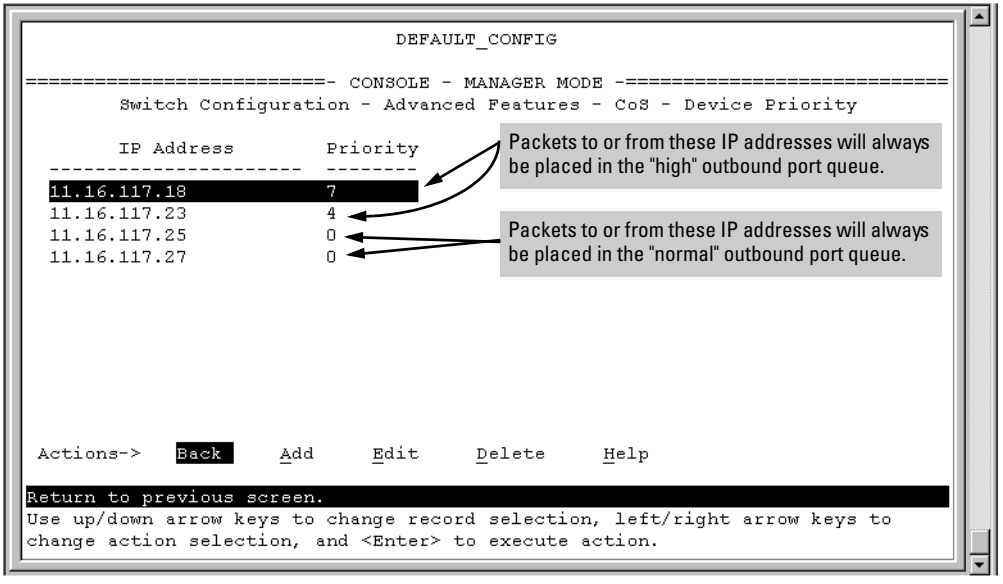

Figure 18. Example of the CoS Device Priority Screen

The Device Priority screen shows examples of CoS device priority configurations. The priorities for IP packets to or from the listed devices will always be controlled by these criteria. If packets for the listed devices are outbound in a tagged VLAN environment, then they will carry with them an 802.1p priority that matches the Priority assignment in this screen.

The CoS Type of Service (ToS) Priority Screen

This feature applies only to IP traffic. CoS reads the Type of Service field in IP packets received from other devices and prioritizes the packets accordingly, unless the same traffic has already been prioritized by the Device Priority (IP address) option. For more information on using ToS criteria, refer to “Using Type of Service (ToS) Criteria to Prioritize IP Traffic” on page 33.

The CoS Protocol Priority Screen

CoS uses protocol criteria to determine traffic priority unless the same traffic has other CoS criteria (configured in other CoS screens) that has a higher precedence. (For precedence information, see Table 5, “Priority Criteria and Precedence,” on page 25.)

To display the Protocol Priority screen, select **Protocol Priority** in the CoS Menu screen (page 29).

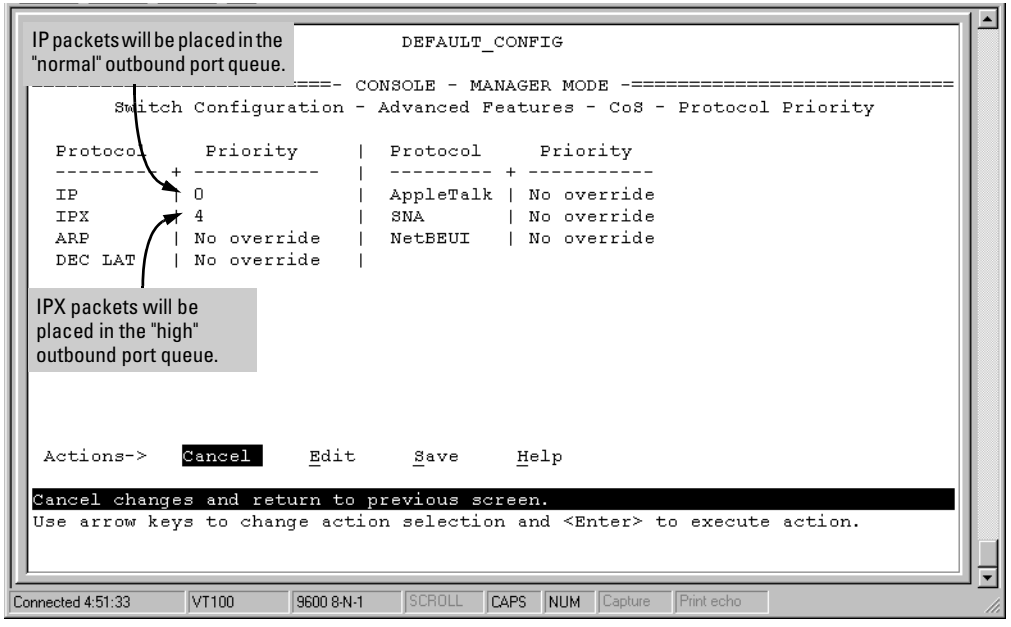

Figure 19. Examples of CoS Protocol Priority Configurations

Where a packet in a listed protocol is outbound in a tagged VLAN environment, then it carries with it an 802.1p priority. If a 0-7 priority is configured, the packet carries the equivalent 802.1p priority. If **No override** is configured, and the packet entered the switch through a tagged VLAN, then the packet carries the 802.1p priority it carried when entering the switch. If **No override** is configured and the packet did not enter the switch through a tagged VLAN, then the packet carries an 802.1p priority of 0 (normal priority) when it leaves the switch.

The CoS VLAN Priority Screen

If you configure CoS on this screen, CoS uses the criteria you specify per VLAN to determine traffic prioritization unless the same traffic has other CoS criteria (configured in other CoS screens) that has a higher precedence. (For precedence information, see table 5, “Priority Criteria and Precedence”, on page 25.)

To display the VLAN Priority screen, select **VLAN Priority** in the CoS Menu screen (page 29).

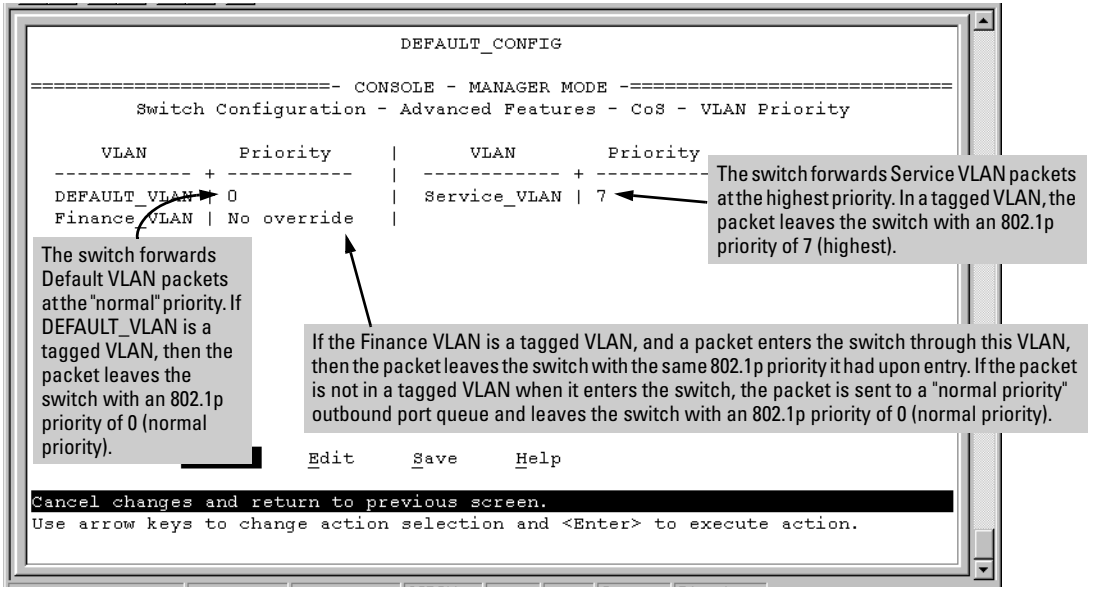

Figure 20. The CoS VLAN Priority Screen

Using Type of Service (ToS) Criteria to Prioritize IP Traffic

Every IP packet includes a Type of Service (ToS) field. This field carries priority settings that are read and used, but not altered by the switch. When CoS is configured to use ToS criteria, the switch reads the content of the packet's ToS field and takes actions based on any CoS configuration that applies to the packet.

In order to use ToS to configure priority, you need to anticipate the ToS field settings in IP packets entering the switch from upstream devices. This involves having knowledge of how an upstream device or application will set the bits in the ToS field of IP packets sent to the switch.

The switch can use the ToS field in either of two ways:

- Use the Differentiated Services bits to select the packets to prioritize (ToS Differentiated Services option)
- Use the Precedence bits to prioritize a packet (ToS IP precedence option).

The following shows an example of the ToS field in the header for an IP packet, and illustrates the diffserve bits and precedence bits in the ToS field. (Note that the Differentiated Services bits and the Precedence bits are two different interpretations of the same field.)

Field:	Destination MAC Address	Source MAC Address	IP Identifier	Type & Version	ToS Byte	. . .
Packet:	FF FF FF FF FF FF	08 00 09 00 00 16	08 00	45	**E0**	. . .

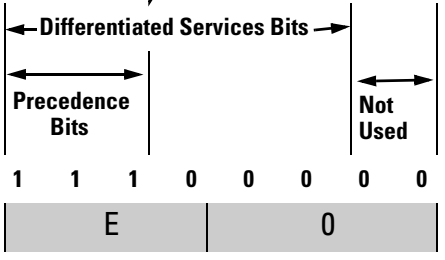

Figure 21. The ToS Field (or Byte) in an IP Header

ToS Configuration Options. To display the Type of Service screen, select **Type of Service (IP Precedence, Differentiated Services)** in the CoS Menu screen (page 29).

Type of Service includes three possible settings:

- **Disabled (the default):** ToS is disabled and is not a factor in prioritizing packets. (Priority settings in the ToS fields of IP packets received by the switch are ignored.)
- **IP Precedence:** ToS is enabled and the switch uses ToS precedence bits (the upper three bits in theToS field) to determine packet priority. The value of these bits are in the range of 0 through 7.
- **Differentiated Services:** ToS is enabled and the switch uses the Differentiated Services bits (the upper six bits) of the ToS field. Each possible setting is termed a codepoint, and there are 64 possible codepoints. This means that you can configure a priority (0 - 7) for up to 64 ToS codepoints. If **No override** is specified for a codepoint, then differentiated services prioritization is not used for packets carrying that codepoint.

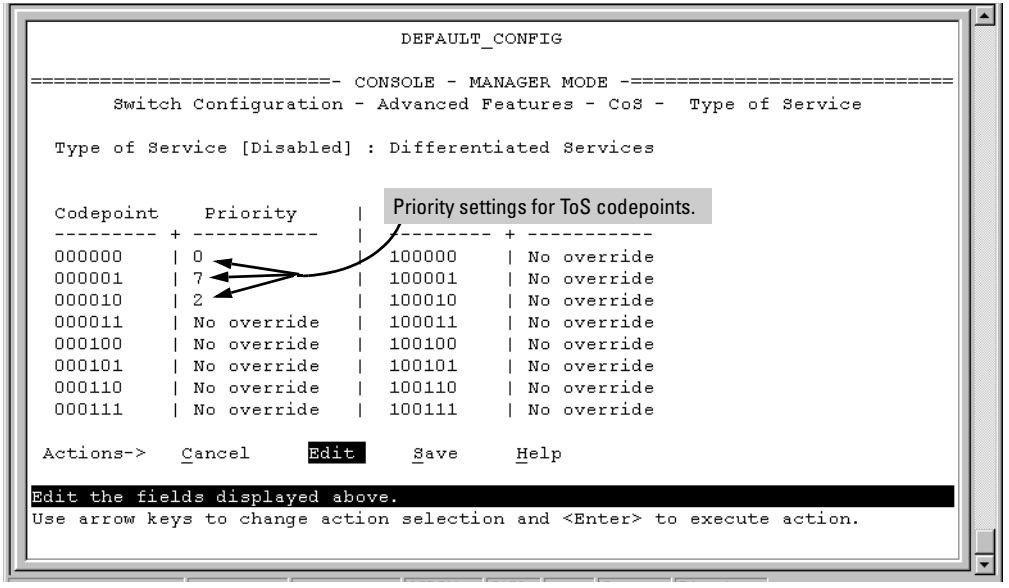

Figure 22. Example of the Differentiated Services (diffserve) Screen

In the above example, the first three ToS codepoints have priority settings. Packets arriving in the switch with these codepoints will be prioritized accordingly (if no higher-precedence CoS criteria apply). That is, a priority of 0 - 3 sends the packet to the normal priority outbound queue. A priority of 4 - 7 sends the packet to the high priority outbound queue. If the packet is outbound in a tagged VLAN, then its 802.1p priority will be set to the same value as the codepoint priority setting (0 - 7).

Table 7. How the Switch Uses the ToS Configuration

Outbound Port	ToS Option:	
	IP Precedence (Value = 0 - 7)	Differentiated Services
IP Packet in an Untagged VLAN or No VLAN	Depending on the value of the IP Precedence bits in the packet's ToS field, the packet will go to either the high or normal priority outbound port queue in the switch: 0 - 3 = normal priority 4 - 7 = high priority	For a given packet carrying a given codepoint in the ToS field: • If a priority (0 - 7) has been configured for that codepoint, the packet will go to either the high or normal priority outbound port queue in the switch: 0 - 3 = normal priority 4 - 7 = high priority • If **No override** (the default) has been configured for that codepoint, then the packet is not prioritized by ToS.
IP Packet in a Tagged VLAN	Same as above, plus the IP Precedence value (0 - 7) will be used to set a corresponding 802.1p priority in the VLAN tag carried by the packet to the next downstream device.	Same as above, plus the user-configured Priority value (0 - 7) will be used to set a corresponding 802.1p priority in the VLAN tag carried by the packet to the next downstream device.

IP Multicast (IGMP) Interaction with CoS

The switch's ability to prioritize IGMP traffic for either a normal or high priority outbound queue overrides any CoS criteria, and does not affect any 802.1p priority settings the switch may assign. For a given packet, if both IGMP high priority and CoS are configured, the CoS configuration overrides the IGMP setting.

IGMP High Priority Configured	CoS Configuration Affects Packet	Switch Port Output Queue	Outbound 802.1p Setting (Requires Tagged VLAN)
Not Enabled	No	Normal	Same as Inbound Setting
Not Enabled	Yes: High Priority (4 - 7)	High	Configured by CoS (4 - 7)
Not Enabled	Yes: Normal Priority (0 - 3)	Normal	Configured by CoS (0 - 3)
Enabled	No	High	Same as Inbound Setting
Enabled	Yes: High Priority (4 - 7)	High	Configured by CoS (4 - 7)
Enabled	Yes: Normal Priority (0 - 3)	High	Configured by CoS (0 - 3)

Summary of CoS Operation

Each of the following four tables provide a hierarchy of CoS criteria and resulting operation, based on one of the four possible tagged VLAN scenarios a packet can encounter while traversing the switch. These scenarios include:

- The packet enters the switch and exits from the switch on a non-VLAN or untagged VLAN port.
- The packet enters the switch in an untagged VLAN and exits from the switch in a tagged VLAN.
- The packet enters the switch in a tagged VLAN and exits from the switch in an untagged VLAN.
- The packet enters the switch and exits from the switch in a tagged VLAN.

In each scenario, only the *first* CoS criteria that applies to a packet is used. All others are ignored.

Packet Enters Switch: On a Non-VLAN Port or in an Untagged VLAN **Packet Exits From Switch: On a Non-VLAN Port or in an Untagged VLAN** **(Prioritizing affects only the choice of outbound priority queue. The packet carries no 802.1p priority tag.)**
1. Device Priority (IP Address) Option *(IP Packets Only)*: – If Device Priority does not apply to the packet, then packet priority defers to the ToS policy. – If Device Priority (0 - 7) is configured and applies to a packet, the packet is assigned to the appropriate queue (high or normal priority) of the outbound port, regardless of any other CoS-configured policy. 2. Type of Service (ToS) Option *(IP Packets Only)*: – If ToS option is configured to **Disabled**, then packet priority defers to the Protocol Priority policy. – IP Precedence option: Prioritizes packet (high or normal) according to the value of the ToS precedence bits (upper three bits of ToS field; 0 - 7); 4 - 7 = high, 0 - 3 = normal. – Differentiated Services option: Prioritizes packet (high or normal) according to Priority setting (0 - 7) for packet's ToS field codepoint. If Priority is set to **No override** (the default), then packet priority defers to the Protocol Priority policy. See "Using Type of Service (ToS) Criteria to Prioritize IP Traffic" on page 33. 3. Protocol Priority Option: – If Protocol Priority does not assign a priority to the packet, then packet priority defers to the VLAN ID policy. – If Protocol Priority assigns a priority (0 - 7) to a packet, the packet is assigned to the appropriate queue (high or normal priority) of the outbound port. 4. VLAN Priority Option: – If VLAN Priority does not assign a priority to the packet, then the packet goes to the "normal" priority queue of an outbound port. – If VLAN Priority assigns a priority (0 - 7) to a packet, the packet is assigned to the appropriate queue (high or normal priority) of the outbound port. (An outbound packet belonging to an untagged VLAN can be assigned to a high or normal priority queue, but cannot be assigned an 802.1p priority because there is no tagged VLAN field in the packet.)

Packet Enters Switch: **In an Untagged VLAN**
Packet Exits From Switch: **In a tagged VLAN**

(Prioritizing affects both the choice of outbound priority queue and the packet's 802.1p priority tag.)

In this scenario, the outbound packet always carries a tagged VLAN field with an 802.1p priority setting.

1. Device Priority (IP Address) Option *(IP Packets Only)*:
   - If Device Priority does not apply to the packet, then packet priority defers to the ToS policy.
   - If Device Priority (0 - 7) is configured and applies to a packet, then the packet is assigned to the appropriate queue (high or normal priority) of the outbound port and the priority value is configured in the 802.1p priority tag in the packet's tagged VLAN field.
2. Type of Service (ToS) Option *(IP Packets Only)*:
   - If ToS option is configured to **Disabled**, then packet priority defers to the Protocol Priority policy.
   - IP Precedence option: Prioritizes packet (high or normal) according to the value of the ToS precedence bits (upper three bits of ToS field; 0 - 7); 4 - 7 = high, 0 - 3 = normal. Also, the Precedence bits are used as follows to configure the 802.1p priority tag in the packet's tagged VLAN field:

IP Precedence Setting:	0	1	2	3	4	5	6	7
802.1p Priority Setting*:	1	2	0	3	4	5	6	7

*To interpret these settings, see Table 4, "Mapping Priority Settings to Device Queues," on page 24.

   - Differentiated Services option: Prioritizes packet (high or normal) according to Priority you set (0 - 7) for the packet's ToS field codepoint. Also, the 802.1p priority tag in the packet's tagged VLAN field is configured to the same value as the Priority you set for the ToS field codepoint. If Priority is set to **No override** (the default), then packet priority defers to the Protocol Priority policy.

See "Using Type of Service (ToS) Criteria to Prioritize IP Traffic" on page 33.

3. Protocol Priority Option:
   - If Protocol Priority does not assign a priority to the packet, then packet priority defers to the VLAN ID policy.
   - If Protocol Priority assigns a priority (0 - 7) to a packet, the packet is assigned to the appropriate queue (high or normal priority) of the outbound port and the priority value is configured in the 802.1p priority tag in the packet's tagged VLAN field.
4. VLAN Priority Option:
   - If VLAN Priority does not assign a priority to the packet, then the packet goes to the "normal" priority queue of an outbound port.
   - If VLAN Priority assigns a priority (0 - 7) to a packet, the packet is assigned to the appropriate queue (high or normal priority) of the outbound port and the priority value is configured in the 802.1p priority tag in the packet's tagged VLAN field.

Packet Enters Switch: **In a tagged VLAN**
Packet Exits From Switch: **In an Untagged VLAN**

(Prioritizing affects only the choice of outbound priority queue. The 802.1p priority tag carried by the packet when it entered the switch is discarded along with the tagged VLAN field.)

1. Device Priority (IP Address) Policy *(IP Packets Only)*:
   - If Device Priority does not apply to the packet, then packet priority defers to the ToS policy.
   - If Device Priority (0 - 7) is configured and applies to a packet, the packet is assigned to the appropriate queue (high or normal priority) of the outbound port, regardless of any other CoS-configured policy.
2. Type of Service (ToS) Policy *(IP Packets Only)*:
   - If ToS option is configured to **Disabled**, then packet priority defers to the Protocol Priority policy.
   - IP Precedence option: Prioritizes packet (high or normal outbound queue) according to the value of the ToS precedence bits (upper three bits of ToS field; 0 - 7); 4 - 7 = high, 0 - 3 = normal.
   - Differentiated Services option: Prioritizes packet (high or normal outbound queue) according to Priority setting (0 - 7) for packet's ToS field codepoint. If Priority is set to **No override** (the default), then packet priority defers to the Protocol Priority policy.

   See "Using Type of Service (ToS) Criteria to Prioritize IP Traffic" on page 33.
3. Protocol Priority Policy:
   - If Protocol Priority does not assign a priority to the packet, then packet priority defers to the VLAN ID policy.
   - If Protocol Priority assigns a priority (0 - 7) to a packet, the packet is assigned to the appropriate queue (high or normal priority) of the outbound port.
4. VLAN Priority Policy:
   - If VLAN Priority does not assign a priority to the packet, then packet priority defers to the incoming 802.1p priority value. (See "Incoming 802.1p Priority" in Table 5, "Priority Criteria and Precedence," on page 25.)
   - If VLAN Priority assigns a priority (0 - 7) to a packet, the packet is assigned to the appropriate queue (high or normal priority) of the outbound port.

   (An outbound packet belonging to an untagged VLAN can be assigned to an outbound, high or normal priority queue, but cannot be assigned an 802.1p priority because there is no tagged VLAN field in the packet.)

Packet Enters Switch: **In a tagged VLAN**
Packet Exits From Switch: **In a tagged VLAN**

(Prioritizing affects both the choice of outbound priority queue and the packet's 802.1p priority tag.)

In this scenario, the packet always carries a tagged VLAN field with an 802.1p priority setting, both inbound and outbound.

1. Device Priority (IP Address) Option *(IP Packets Only)*:
   - If Device Priority does not apply to the packet, then packet priority defers to the ToS policy.
   - If Device Priority (0 - 7) is configured and applies to a packet, then the packet is assigned to the appropriate queue (high or normal priority) of the outbound port and the priority value is configured in the 802.1p priority tag in the packet's tagged VLAN field. This assignment replaces whatever 802.1p priority tag value the packet had when it entered the switch.

2. Type of Service (ToS) Option *(IP Packets Only)*:
   - If ToS option is configured to **Disabled**, then packet priority defers to the Protocol Priority policy.
   - IP Precedence option: Prioritizes packet (high or normal) according to the value of the ToS precedence bits (upper three bits of ToS field; 0 - 7); 4 - 7 = high, 0 - 3 = normal. Also, the Precedence bits are used as follows to configure the 802.1p priority tag in the packet's tagged VLAN field:

IP Precedence Setting:	0	1	2	3	4	5	6	7
802.1p Priority Setting*:	1	2	0	3	4	5	6	7

*To interpret these settings, see Table 4, "Mapping Priority Settings to Device Queues," on page 24.

     This assignment replaces whatever 802.1p priority tag value that the packet had when it entered the switch.
   - Differentiated Services option: Prioritizes packet (high or normal) according to Priority you set (0 - 7) for the packet's ToS field Codepoint. Also, the 802.1p priority tag in the packet's tagged VLAN field is configured to the same value as the Priority you set for the ToS field Codepoint. This assignment replaces whatever 802.1p priority tag value the packet had when it entered the switch. If Priority is set to **No override** (the default), then packet priority defers to the Protocol Priority policy.

   See "Using Type of Service (ToS) Criteria to Prioritize IP Traffic" on page 33.

3. Protocol Priority Option:
   - If Protocol Priority does not assign a priority to the packet, then packet priority defers to the VLAN ID policy.
   - If Protocol Priority assigns a priority (0 - 7) to a packet, the packet is assigned to the appropriate queue (high or normal priority) of the outbound port and the priority value is configured in the 802.1p priority tag in the packet's tagged VLAN field. This assignment replaces whatever 802.1p priority tag value the packet had when it entered the switch.

4. VLAN Priority Option:
   - If VLAN Priority does not assign a priority to the packet, then packet priority defers to the incoming 802.1p priority value. (See "Incoming 802.1p Priority" in Table 5, "Priority Criteria and Precedence," on page 25.)
   - If VLAN Priority assigns a priority (0 - 7) to a packet, the packet is assigned to the appropriate queue (high or normal priority) of the outbound port and the priority value is configured in the 802.1p priority tag in the packet's tagged VLAN field. This assignment replaces whatever 802.1p priority tag value the packet had when it entered the switch.

Supporting CoS with an 802.1Q Tagged VLAN Environment

Using HP's 802.1Q-compliant switches, you can create either a single tagged VLAN or multiple tagged VLANs. To do either, you need an 802.1Q-compliant device connected to each tagged VLAN port on an HP switch. For more on VLANs, see the *Management and Configuration Guide* you received with the switch (and also available on HP's ProCurve website at **www.hp.com/go/procurve**).

Using the Default VLAN to Create a Single Tagged VLAN

1. Activate the switch's VLAN support. To access the VLAN Support option from the Main Menu, select the following:

   Switch Configuration . . .

   Advanced Features . . .

   VLAN Menu . . .

   Activate VLAN Support

2. From the Main Menu, reboot the switch.
3. In the VLAN Port Assignment screen, reconfigure to **Tagged** every port that is connected to an 802.1Q-compliant device. To access the VLAN Port Assignment screen, select the following:

   Switch Configuration . . .

   Advanced Features . . .

   VLAN Menu . . .

   VLAN Port Assignment

4. Ensure that each 802.1Q-compliant device connected to a port in step 3 is configured as tagged for the default VLAN.

Operating and Troubleshooting Notes

- **For Devices that Do Not Support 802.1Q Tagged VLANs:** For communication between these devices and the switch, connect the device to a switch port configured as **Untagged** for the VLAN in which you want the device's traffic to move.
- **VLAN Tagging Rules:** For a port on the switch to be a member of a VLAN, the port must be configured as either **Tagged** or **Untagged** for that VLAN. (Only one VLAN on a port can be untagged. Otherwise, the switch cannot determine which VLAN should receive untagged VLAN traffic.)
- **Loss of Communication on a Tagged VLAN:** If you cannot communicate with a device in a tagged VLAN environment, ensure that the device either supports tagged VLANs or is connected to a VLAN port that is configured as **Untagged**.

For more on VLANs, refer to the *Management and Configuration Guide* you received with the switch.

Manual Part Number
5969-2305
Edition 2, May 1999