Chapter 6
Global CONFIG Commands

aaa

Defines an authentication-method list for access to a switch or routing switch.

EXAMPLE:

To configure an access method list, enter a command such as the following:

```
HP9300(config)# aaa authentication web-server default local
```

This command configures the device to use the local user accounts to authenticate access to the device through the Web management interface. If the device does not have a user account that matches the user name and password entered by the user, the user is not granted access.

To configure the device to consult a RADIUS server first for Enable access, then consult the local user accounts if the RADIUS server is unavailable, enter the following command:

```
HP9300(config)# aaa authentication enable default radius local
```

Syntax: [no] aaa authentication snmp-server | web-server | enable | login default <method1> [<method2>] [<method3>] [<method4>] [<method5>] [<method6>] [<method7>]

The **snmp-server | web-server | enable | login** parameter specifies the type of access this authentication-method list controls. You can configure one authentication-method list for each type of access.

NOTE: TACACS/TACACS+ and RADIUS are supported only for enable and login.

The <method1> parameter specifies the primary authentication method. The remaining optional <method> parameters specify the secondary methods to try if an error occurs with the primary method. A method can be one of the values listed in the Method Value column in the following table.

Table 6.1: Authentication Method Values

Method Value	Description
tacacs or **tacacs+**	A TACACS/TACACS+ server. You can use either parameter. Each parameter supports both TACACS and TACACS+. You also must identify the server to the device using the **tacacs-server** command.
radius	A RADIUS server. You also must identify the server to the device using the **radius-server** command.

Table 6.1: Authentication Method Values (Continued)

Method Value	Description
local	A local user name and password you configured on the device. Local user names and passwords are configured using the **username…** command.
line	The password you configured for Telnet access. The Telnet password is configured using the **enable telnet password…** command.
enable	The super-user "enable" password you configured on the device. The enable password is configured using the **enable super-user-password…** command.
none	No authentication is used. The device automatically permits access.

Possible values: see above

Default value: N/A

access-list (standard)

Configures standard Access Control Lists (ACLs), which permit or deny packets based on source IP address (in contrast to extended ACLs, which permit or deny packets based on source and destination IP address and also based on IP protocol information). You can configure up to 99 standard ACLs. You can configure up to 1024 individual ACL entries. There is no limit to the number of ACL entries an ACL can contain except for the system-wide limitation of 1024 total ACL entries.

EXAMPLE:

To configure a standard ACL and apply it to outgoing traffic on port 1/1, enter the following commands.

```
HP9300(config)# access-list 1 deny host 209.157.22.26 log
HP9300(config)# access-list 1 deny 209.157.29.12 log
HP9300(config)# access-list 1 deny host IPHost1 log
HP9300(config)# access-list 1 permit any
HP9300(config)# int eth 1/1
HP9300(config-if-1/1)# ip access-group 1 out
HP9300(config-if-1/1)# write mem
```

The commands in this example configure an ACL to deny packets from three source IP addresses from being forwarded on port 1/1. The last ACL entry in this ACL permits all packets that are not explicitly denied by the first three ACL entries.

Syntax: [no] access-list <num> deny | permit <source-ip> | <hostname> <wildcard> [log]

Syntax: [no] access-list <num> deny | permit <source-ip> | <hostname>/<mask-bits> [log]

Syntax: [no] access-list <num> deny | permit host <source-ip> | <hostname> [log]

Syntax: [no] access-list <num> deny | permit any [log]

Syntax: [no] ip access-group <num> in | out

The <num> parameter is the access list number and can be from 1 – 99.

The **deny | permit** parameter indicates whether packets that match a policy in the access list are denied (dropped) or permitted (forwarded).

The <source-ip> parameter specifies the source IP address. Alternatively, you can specify the host name.

NOTE: To specify the host name instead of the IP address, the host name must be configured using the HP device's DNS resolver. To configure the DNS resolver name, use the **ip dns server-address…** command at the global CONFIG level of the CLI.

The <wildcard> parameter specifies the mask value to compare against the host address specified by the <source-ip> parameter. The <wildcard> is a four-part value in dotted-decimal notation (IP address format) consisting of ones and zeros. Zeros in the mask mean the packet's source address must match the <source-ip>. Ones mean any value matches. For example, the <source-ip> and <wildcard> values 209.157.22.26 0.0.0.255 mean that all hosts in the Class C sub-net 209.157.22.x match the policy.

If you prefer to specify the wildcard (mask value) in CIDR format, you can enter a forward slash after the IP address, then enter the number of significant bits in the mask. For example, you can enter the CIDR equivalent of "209.157.22.26 0.0.0.255" as "209.157.22.26/24".

NOTE: When you save ACL policies to the startup-config file, the software changes your <source-ip> values if appropriate to contain zeros where the packet value must match. For example, if you specify 209.157.22.26/24 or 209.157.22.26 255.255.255.0, then save the startup-config file, the values appear as 209.157.22.0/24 (if you have enabled display of sub-net lengths) or 209.157.22.0 255.255.255.0 in the startup-config file.

If you enable the software to display IP sub-net masks in CIDR format, the mask is saved in the file in "/<mask-bits>" format. To enable the software to display the CIDR masks, enter the **ip show-subnet-length** command at the global CONFIG level of the CLI. You can use the CIDR format to configure the ACL entry regardless of whether the software is configured to display the masks in CIDR format.

NOTE: If you use the CIDR format, the ACL entries appear in this format in the running-config and startup-config files, but are shown with sub-net mask in the display produced by the **show access-list** and **show ip access-list** commands.

The **host** <source-ip> | <hostname> parameter lets you specify a host IP address or name. When you use this parameter, you do not need to specify the mask. A mask of all zeros (0.0.0.0) is implied.

The **any** parameter configures the policy to match on all host addresses.

The **log** argument configures the device to generate Syslog entries and SNMP traps for packets that are permitted or denied by the access policy.

The **in | out** parameter specifies whether the ACL applies to incoming traffic or outgoing traffic on the port to which you apply the ACL.

Possible values: see above

Default value: N/A

access-list (extended)

Configures extended ACLs, which permit or deny packets based on the following information:

- IP protocol
- Source IP address or host name
- Destination IP address or host name
- Source TCP or UDP port (if the IP protocol is TCP or UDP)
- Destination TCP or UDP port (if the IP protocol is TCP or UDP)

EXAMPLE:

To configure an extended ACL that blocks all Telnet traffic received on port 1/1 from IP host 209.157.22.26, enter the following commands.

```
HP9300(config)# access-list 101 deny tcp host 209.157.22.26 any eq telnet log
HP9300(config)# access-list 101 permit ip any any
HP9300(config)# int eth 1/1
HP9300(config-if-1/1)# ip access-group 101 in
HP9300(config)# write mem
```

Syntax: access-list <num> deny | permit <ip-protocol> <source-ip> | <hostname> <wildcard> [<operator> <source-tcp/udp-port>] <destination-ip> | <hostname> <wildcard> [<operator> <destination-tcp/udp-port>] [precedence <name> | <num>] [tos <name> | <num>] [log]

Syntax: [no] access-list <num> deny | permit host <ip-protocol> any any [log]

Syntax: [no] ip access-group <num> in | out

The <num> parameter indicates the ACL number and can be from 100 – 199 for an extended ACL.

The **deny | permit** parameter indicates whether packets that match the policy are dropped or forwarded.

The <ip-protocol> parameter indicates the type of IP packet you are filtering. You can specify one of the following:

- **icmp**
- **igmp**
- **igrp**
- **ip**
- **ospf**
- **tcp**
- **udp**

The <source-ip> | <hostname> parameter specifies the source IP host for the policy. If you want the policy to match on all source addresses, enter **any**.

The <wildcard> parameter specifies the portion of the source IP host address to match against. The <wildcard> is a four-part value in dotted-decimal notation (IP address format) consisting of ones and zeros. Zeros in the mask mean the packet's source address must match the <source-ip>. Ones mean any value matches. For example, the <source-ip> and <wildcard> values 209.157.22.26 0.0.0.255 mean that all hosts in the Class C sub-net 209.157.22.x match the policy.

If you prefer to specify the wildcard (mask value) in Classless Interdomain Routing (CIDR) format, you can enter a forward slash after the IP address, then enter the number of significant bits in the mask. For example, you can enter the CIDR equivalent of "209.157.22.26 0.0.0.255" as "209.157.22.26/24".

NOTE: When you save ACL policies to the startup-config file, the software changes your IP address values if appropriate to contain zeros where the packet value must match. For example, if you specify 209.157.22.26/24 or 209.157.22.26 255.255.255.0, then save the startup-config file, the values appear as 209.157.22.0/24 (if you have enabled display of sub-net lengths) or 209.157.22.0 255.255.255.0 in the startup-config file.

If you enable the software to display IP sub-net masks in CIDR format, the mask is saved in the file in "/<mask-bits>" format. To enable the software to display the CIDR masks, enter the **ip show-subnet-length** command at the global CONFIG level of the CLI. You can use the CIDR format to configure the ACL entry regardless of whether the software is configured to display the masks in CIDR format.

NOTE: If you use the CIDR format, the ACL entries appear in this format in the running-config and startup-config files, but are shown with sub-net mask in the display produced by the **show access-list** and **show ip access-list** commands.

The <destination-ip> | <hostname> parameter specifies the destination IP host for the policy. If you want the policy to match on all destination addresses, enter **any**.

The <operator> parameter specifies a comparison operator for the TCP or UDP port number. This parameter applies only when you specify **tcp** or **udp** as the IP protocol. For example, if you are configuring an entry for HTTP, specify **tcp eq http**. You can enter one of the following operators:

- **eq** – The policy applies to the TCP or UDP port name or number you enter after **eq**.
- **gt** – The policy applies to TCP or UDP port numbers greater than the port number or the numeric equivalent of the port name you enter after **gt**.

- **lt** – The policy applies to TCP or UDP port numbers that are less than the port number or the numeric equivalent of the port name you enter after **lt**.
- **neq** – The policy applies to all TCP or UDP port numbers except the port number or port name you enter after **neq**.
- **range** – The policy applies to all TCP or UDP port numbers that are between the first TCP or UDP port name or number and the second one you enter following the **range** parameter. The range includes the port names or numbers you enter. For example, to apply the policy to all ports between and including 23 (Telnet) and 53 (DNS), enter the following: **range 23 53**. The first port number in the range must be lower than the last number in the range.
- **established** – This operator applies only to TCP packets. If you use this operator, the policy applies to TCP packets that have the ACK (Acknowledgment) or RST (Reset) bits set on (set to "1") in the Control Bits field of the TCP packet header. Thus, the policy applies only to established TCP sessions, not to new sessions. See Section 3.1, "Header Format", in RFC 793 for information about this field.

NOTE: This operator applies only to destination TCP ports, not source TCP ports.

The <TCP/UDP-port> parameter specifies the TCP or UDP port number or well-known name. The device recognizes the following well-known names. For other ports, you must specify the port number.

NOTE: The following lists are organized alphabetically. In the CLI, these port names are listed according to ascending port number.

- TCP port names recognized by the software:
  - bgp
  - dns
  - ftp
  - http
  - imap4
  - ldap
  - nntp
  - pop2
  - pop3
  - smtp
  - ssl
  - telnet
- UDP port names recognized by the software:
  - bootps
  - bootpc
  - dns
  - ntp
  - radius
  - radius-old
  - rip
  - snmp

- snmp-trap
- tftp

The **in | out** parameter specifies whether the ACL applies to incoming traffic or outgoing traffic on the port to which you apply the ACL.

The **precedence** <name> | <num> parameter of the **ip access-list** command specifies the IP precedence. The precedence option for of an IP packet is set in a three-bit field following the four-bit header-length field of the packet's header. You can specify one of the following:

- **critical** or **5** – The ACL matches packets that have the critical precedence. If you specify the option number instead of the name, specify number 5.
- **flash** or **3** – The ACL matches packets that have the flash precedence. If you specify the option number instead of the name, specify number 3.
- **flash-override** or **4** – The ACL matches packets that have the flash override precedence. If you specify the option number instead of the name, specify number 4.
- **immediate** or **2** – The ACL matches packets that have the immediate precedence. If you specify the option number instead of the name, specify number 2.
- **internet** or **6** – The ACL matches packets that have the internetwork control precedence. If you specify the option number instead of the name, specify number 6.
- **network** or **7** – The ACL matches packets that have the network control precedence. If you specify the option number instead of the name, specify number 7.
- **priority** or **1** – The ACL matches packets that have the priority precedence. If you specify the option number instead of the name, specify number 1.
- **routine** or **0** – The ACL matches packets that have the routine precedence. If you specify the option number instead of the name, specify number 0.

The tos <name> | <num> parameter of the **ip access-list** command specifies the IP TOS.

You can specify one of the following:

- **max-reliability** or **2** – The ACL matches packets that have the maximum reliability TOS. The decimal value for this option is 2.
- **max-throughput** or **4** – The ACL matches packets that have the maximum throughput TOS. The decimal value for this option is 4.
- **min-delay** or **8** – The ACL matches packets that have the minimum delay TOS. The decimal value for this option is 8.
- **min-monetary-cost** or **1** – The ACL matches packets that have the minimum monetary cost TOS. The decimal value for this option is 1.
- **normal** or **0** – The ACL matches packets that have the normal TOS. The decimal value for this option is 0.
- <num> – A number from 0 – 15 that is the sum of the numeric values of the options you want. The TOS field is a four-bit field following the Precedence field in the IP header. You can specify one or more of the following. To select more than one option, enter the decimal value that is equivalent to the sum of the numeric values of all the TOS options you want to select. For example, to select the max-reliability and min-delay options, enter number 10. To select all options, select 15.

The **log** parameter enables SNMP traps and Syslog messages for packets denied by the ACL.

Possible values: see above

Default value: N/A

all-client

Restricts management access to the HP device to the host whose IP address you specify. No other device except the one with the specified IP address can access the HP device through Telnet (CLI), the Web (Web management interface), or SNMP.

If you want to restrict access for some of the management platforms but not all of them, use one or two of the following commands:

- **snmp-client** – restricts all SNMP access. See “snmp-client” on page 6-56.
- **telnet-client** – restricts Telnet access. See “telnet-client” on page 6-63.
- **web-client** – restricts web access. See “web-client” on page 6-66.

EXAMPLE:

To restrict all management access to the HP device to the host with IP address 209.157.22.26, enter the following command:

```
HP9300(config)# all-client 209.157.22.26
```

Syntax: [no] all-client <ip-addr>

Possible values: a valid IP address. You can enter one IP address with the command. You can use the command up to ten times for up to ten IP addresses.

Default value: N/A

appletalk arp-age

Defines how long an AppleTalk ARP entry will remain active before being aged out.

EXAMPLE:

```
HP9300(config)# appletalk arp-age 115
```

Syntax: appletalk arp-age <1 – 240>

Possible values: 1 – 240 minutes

Default value: 10 minutes

appletalk arp retransmit-count

Allows you to modify the maximum number of times that a packet will be sent out for ARP cache informational updates. The packet will be sent out to the maximum amount defined, until the information is received.

If no response is received before the count number expires, no additional packets will be sent.

EXAMPLE:

To modify the number of times packet requests will be sent out for ARP updates from the default value of 2 to 8, enter the following:

```
HP9300(config)# appletalk arp retransmit-count 8
```

Syntax: appletalk arp retransmit-count <value>

Possible values: 1 – 10

Default value: 2

appletalk arp retransmit-interval

Allows you to modify the interval between the transmission of ARP packets.

EXAMPLE:

To modify the retransmission interval from the default value of 1 to 15 seconds, enter the following:

```
HP9300(config)# appletalk arp retransmit-interval 15
```

Syntax: appletalk arp retransmit-interval <value>

Possible values:1 – 120 seconds

Default value: 1

appletalk glean-packets

When the glean packet parameter is enabled on an AppleTalk router, it will try to learn the MAC address from the packet instead of sending out an AARP request.

EXAMPLE:

To enable glean packets on an AppleTalk router, enter the following:

```
HP9300(config)# appletalk glean-packets
```

Syntax: appletalk glean-packets

Possible values: enabled or disabled

Default value: disabled

appletalk qos socket

You can use the Quality of Service (QoS) socket parameter to assign a higher priority to specific AppleTalk sockets. Enter a value from 0 – 7.

For information about HP QoS, see the “Quality of ServIce (QoS)” chapter in the *Advanced Configuration and Management Guide*.

EXAMPLE:

To assign socket 123 to the premium queue, enter the following command:

```
HP9300(config)# appletalk qos socket 123 priority 7
```

Syntax: [no] appletalk qos socket <num> | all priority <num>

Possible values: The first <num> parameter specifies the socket number.

The **all** option specifies all sockets.

The second <num> parameter can be from 0 – 7 and specifies the IEEE 802.1 equivalent to one of the four QoS queues.

Default value: By default, all AppleTalk sockets are in the best effort queue (qosp0).

appletalk rtmp-update-interval

Allows you to modify how often RTMP updates are sent out on AppleTalk interfaces.

EXAMPLE:

To change the value to 50 seconds from a default value of 10 seconds, enter the following:

```
HP9300(config)# appletalk rtmp-update-interval 50
```

Syntax: appletalk rtmp-update-interval <seconds>

Possible values: 1 – 3600 seconds

Default value: 10 seconds

appletalk zip-query-interval

EXAMPLE:

To change the ZIP query interval to 30 seconds from a default value of 10 seconds, enter the following:

```
HP9300(config)# appletalk zip-query-interval 30
```

Syntax: appletalk zip-query-interval <seconds>

Possible values: 1 – 1000 seconds

Default value: 10 seconds

arp

Enters a static IP ARP entry for static routes on an HP router. This command is not available on HP switches.

EXAMPLE:

```
HP9300(config)# arp 1 192.53.4.2 1245.7654.2348 e 4/11
```

Syntax: arp <num> <ip-addr> <mac-addr> ethernet <portnum>

Possible values: The maximum number of ARP entries you can add depends on the device. To display the maximum number you can configure on your device, enter the **show default values** command and look at the row of information for the ip-arp parameter. See “show default” on page 20-6.

Default value: N/A

boot system bootp

Initiates a system boot from a BootP server. You can specify the preferred initial boot source and boot sequence in the startup-config file. If upon boot, the user-specified boot source and sequence fails then by default, the switch or router will attempt to load the software image from a different source. The following sources will be tried one at a time, in the order noted, until a software load is successful.

- flash primary
- flash secondary
- bootp

If the image does not load successfully from the above sources, you are prompted to enter alternative locations from which to load an image:

- boot system bootp
- boot system flash primary
- boot system flash secondary
- boot system tftp

EXAMPLE:

```
HP9300(config)# boot sys bootp
```

Syntax: boot system bootp

Possible values: N/A

Default value: N/A

boot system flash primary

Initiates a system boot of the primary software image stored in flash.

EXAMPLE:

```
HP9300(config)# boot sys fl pri
```

Syntax: boot system flash primary

Possible values: N/A

Default value: N/A

boot system flash secondary

Initiates a system boot of the secondary software image stored in flash.

EXAMPLE:

```
HP9300(config)# boot sys fl sec
```

Syntax: boot system flash secondary

Possible values: N/A

Default value: N/A

boot system tftp

Initiates a system boot of the software image from a TFTP server.

EXAMPLE:

```
HP9300(config)# boot sys tftp 192.22.33.44 current.img
```

NOTE: Before entering the TFTP boot command, you must first assign an **IP address**, **IP mask**, and **default gateway** (if applicable) at the boot prompt as shown.

EXAMPLE:

```
boot> ip address 192.22.33.44 255.255.255.0
boot> ip default-gateway 192.22.33.1
```

You now can proceed with the **boot system tftp…** command.

Syntax: boot system tftp <ip-addr> <filename>

Possible values: N/A

Default value: N/A

NOTE: See the “Updating Software Images and Configuration Files” chapter of the *Installation and Getting Started Guide* for more information regarding software and configuration file transfers and updates.

bootp-relay-max-hops

Defines the maximum number of hops that a BootP request will be allowed to traverse before being dropped.

EXAMPLE:

```
HP9300(config)# bootp-relay-max-hops 5
```

Syntax: bootp-relay-max-hops <value>

Possible values: 1 – 15

Default value: 4

broadcast filter

Configures a Layer 2 broadcast packet filter. You can filter on all broadcast traffic or on IP UDP broadcast traffic.

EXAMPLE:

To configure a Layer 2 broadcast filter to filter all types of broadcasts, then apply the filter to ports 1/1, 1/2, and 1/3, enter the following commands:

```
HP9300(config)# broadcast filter 1 any
HP9300(config-bcast-filter-id-1)# exclude-ports ethernet 1/1 to 1/3
HP9300(config-bcast-filter-id-1)# write mem
```

EXAMPLE:

To configure two filters, one to filter IP UDP traffic on ports 1/1 – 1/4, and the other to filter all broadcast traffic on port 4/6, enter the following commands:

```
HP9300(config)# broadcast filter 1 ip udp
HP9300(config-bcast-filter-id-1)# exclude-ports ethernet 1/1 to 1/4
HP9300(config-bcast-filter-id-1)# exit
```

```
HP9300(config)# broadcast filter 2 any
HP9300(config-bcast-filter-id-2)# exclude-ports ethernet 4/6
HP9300(config-bcast-filter-id-2)# write mem
```

EXAMPLE:

To configure an IP UDP broadcast filter and apply that applies only to port-based VLAN 10, then apply the filter to two ports within the VLAN, enter the following commands:

```
HP9300(config)# broadcast filter 4 ip udp vlan 10
HP9300(config-bcast-filter-id-4)# exclude-ports eth 1/1 eth 1/3
HP9300(config-bcast-filter-id-1)# write mem
```

Syntax: [no] broadcast filter <filter-ID> any | ip udp [vlan <vlan-id>]

The <filter-ID> specifies the filter number and can a number from 1 – 8. The software applies the filters in ascending numerical order. As soon as a match is found, the software takes the action specified by the filter (block the broadcast) does not compare the packet against additional broadcast filters.

You can specify **any** or **ip udp** as the type of broadcast traffic to filter. The **any** parameter prevents all broadcast traffic from being sent on the specified ports. The **ip udp** parameter prevents all IP UDP broadcasts from being sent on the specified ports but allows other types of broadcast traffic.

If you specify a port-based VLAN ID, the filter applies only to the broadcast domain of the specified VLAN, not to all broadcast domains (VLANs) on the device.

As soon as you press Enter after entering the command, the CLI changes to the configuration level for the filter you are configuring. You specify the ports to which the filter applies at the filter's configuration level.

Syntax: [no] exclude-ports ethernet <portnum> to <portnum>

Or

Syntax: [no] exclude-ports ethernet <portnum> ethernet <portnum>

These commands specify the ports to which the filter applies.

NOTE: This is the same command syntax as that used for configuring port-based VLANs. Use the first command for adding a range of ports. Use the second command for adding separate ports (not in a range). You also can combine the syntax. For example, you can enter **exclude-ports ethernet 1/4 ethernet 2/6 to 2/9**.

Possible values: see above

Default value: N/A

broadcast limit

Specifies the maximum number of broadcast packets the device can forward each second. By default the device sends broadcasts and all other traffic at wire speed and is limited only by the capacities of the hardware. However, if other devices in the network cannot handle unlimited broadcast traffic, this command allows you to relieve those devices by throttling the broadcasts at the HP device.

NOTE: The broadcast limit does not affect multicast or unicast traffic. However, you can use the **multicast limit** and **unknown-unicast limit** commands to control these types of traffic. See “multicast limit” on page 6-44 and “unknown-unicast limit” on page 6-65.

EXAMPLE:

```
HP9300(config)# broadcast limit 30000
```

Syntax: broadcast limit <num>

Possible values: 0 – 4294967295

Default value: N/A

chassis name

Assigns a name to a Chassis device. It is similar to the **hostname** command used for Fixed-port devices.

Assign a host name to an HP 9304M or HP 9308M Chassis device to more easily manage it. By default, an HP 9304M will be identified as “HP9304” and an HP 9308M will be identified as “HP9308” in the CLI command prompt.

EXAMPLE:

To change the name of a Chassis device to RouterNYC from the system default, enter the following:

```
HP9300(config)# chassis name routernyc
Routernyc(config)#
```

Syntax: chassis name <text>

Possible values: Up to 32 alphanumeric characters can be assigned to hostname text string.

Default value: HP9304 or HP9308

chassis poll-time

Changes the number of seconds between polls of the power supply, fan, and temperature status.

Use the **show chassis** command to display the hardware status.

EXAMPLE:

To change the hardware poll time from 60 seconds (the default) to 30 seconds:

```
HP9300(config)# chassis poll-time 30
```

Syntax: chassis poll-time <num>

Possible values: 0 – 65535

Default value: 60

chassis trap-log

Disables or re-enables status polling for individual power supplies and fans. When you disable status polling, a fault in the power supply does not generate a trap in the system log.

EXAMPLE:

To disable polling of power supply 2, enter the following command:

```
HP9300(config)# no chassis trap-log ps2
```

Syntax: [no] chassis trap-log ps1 | ps2 | ps3 | ps4 | fan1 | fan2 | fan3 | fan4

Possible values: see above

Default value: all traps enabled

clock summer-time

Causes daylight savings time to be automatically activated and deactivated for the relevant time zones.

EXAMPLE:

```
HP9300# clock summer-time
```

Syntax: clock summer-time

Possible values: N/A

Default value: N/A

clock timezone

Allows you to define the time zone of the clock. This parameter is used in conjunction with the **clock set** command or for timestamps obtained from an SNTP server. The **clock set...** command is configured at the privileged EXEC level of the CLI.

NOTE: Use this **clock** command before all others to ensure accuracy of the clock settings.

NOTE: For those time zones that recognize daylight savings time, the **clock summer-time** command will also need to be defined.

NOTE: Clock settings are not saved over power cycles; however, you can configure the system to reference an SNTP server at power up. This server will then automatically download the correct time reference for the network. The local switch and router will then adjust the time according to its time zone setting. For more details on setting up an SNTP reference clock, refer to the **sntp** command at the privileged EXEC level and the **sntp poll-interval** and **sntp server** commands at the global CONFIG level.

EXAMPLE:

```
HP9300# clock timezone us eastern
```

Syntax: clock timezone gmt | us <timezone>

Possible values: The following time zones can be entered for US or GMT:

- US time zones: alaska, aleution, arizona, central, east-indiana, eastern, hawaii, michigan, mountain, pacific, samoa
- GMT time zones: gmt+12, gmt+11, gmt+10...fmt+01, gmt+00, gmt-01...gmt-10, gmt-11, gmt-12

Default value: pacific

confirm-port-up

Reduces the number of up-status confirmations the software requires before bringing a port up for use. This command is useful for network interface cards (NICs) that are designed to come up very quickly in certain applications and are sensitive to the slight delay caused by the HP ports as they wait for the multiple status indications before coming up. You can configure an HP device to reduce the number of status indications the software requires before bringing up a 10/100Base-Tx port.

NOTE: Do not use this command unless advised to do so by HP technical support.

By default, HP devices wait for multiple indications that a port is good before bringing the port up. Specific types of networking devices are sensitive to the very slight delay caused by the multiple status indications. In this case, you can use one of the following methods to reduce the number of status indications the software requires before bringing up a 10/100Base-Tx port.

You also can set this parameter on individual ports.

EXAMPLE:

By default, the devices bring a 10/100 Base-Tx port up after receiving three consecutive up-status indications for the port. You can reduce this number to just one indication. To reduce the up-status indications required to bring up 10/100 ports 1/1 – 1/8 to just one, enter the following commands:

```
HP9300(config)# int ethernet 1/1 to 1/8

HP9300(config-mif-1/1-1/8) confirm-port-up 1

HP9300(config-mif-1/1-1/8) write mem
```

Syntax: [no] confirm-port-up <num>

The <num> parameter specifies the number of indications required by the software and can be from 1 – 10. The default is 3.

Possible values: 1 – 10

Default value: 3

console

Times out idle serial management sessions.

By default, an HP device does not time out serial CLI sessions. A serial session remains open indefinitely until you close it. You can configure the device to time out serial CLI sessions if they remain idle for a specified number of minutes. You can configure an idle timeout value from 0 – 240 minutes. The default is 0.

NOTE: If a session times out, the device does not close the connection. Instead, the CLI changes to the User EXEC mode (for example: HP9300>).

EXAMPLE:

To configure the idle timeout for serial CLI sessions, enter a command such as the following:

```
HP9300(config)# console timeout 20
```

This command configures the idle timeout value to 20 minutes.

Syntax: [no] console timeout <num>

The <num> parameter specifies the number of minutes the serial CLI session can remain idle before it times out. You can specify from 0 – 240 minutes. The default is 0 (sessions never time out).

Possible values: 0 – 240 minutes

Default value: 0 (sessions never time out)

default-vlan-id

When you enable port-based VLAN operation, all ports are assigned to VLAN 1 by default. As you create additional VLANs and assign ports to them, the ports are removed from the default VLAN. All ports that you do not assign to other VLANs remain members of default VLAN 1. This behavior ensures that all ports are always members of at least one VLAN.

You can change the VLAN ID for the default VLAN by entering the following command at the global CONFIG level of the CLI:

```
HP9300(config)# default-vlan-id 4095
```

You must specify a valid VLAN ID that is not already in use. For example, if you have already defined VLAN 10, do not try to use "10" as the new VLAN ID for the default VLAN. Valid VLAN IDs are numbers from 1 – 4095.

NOTE: Changing the default VLAN name does not change the properties of the default VLAN. Changing the name allows you to use the VLAN ID "1" as a configurable VLAN.

dhcp-gateway-list

This parameter must be defined when the feature, DHCP Assist, is enabled on an HP switch. A gateway address must be defined for each sub-net that will be requesting addresses from a DHCP server. This allows the stamping process to occur. Each gateway address defined on the switch corresponds to an IP address of the HP router interface or other router involved.

Up to eight addresses can be defined for each gateway list in support of ports that are multi-homed. When multiple IP addresses are configured for a gateway list, the switch inserts the addresses into the discovery packet in a round robin fashion.

Up to 32 gateway lists can be defined for each switch.

NOTE: For more details on this command and the DHCP Assist feature, see the “Configuring Basic Features” chapter of the *Installation and Getting Started Guide*.

EXAMPLE:

To define the sub-net address 192.95.5.1 as a gateway address and assign it to interface 4, enter the following:

```
HP6208(config)# dhcp-gateway-list 1 192.95.5.1
```

```
HP6208(config)# int e 4
HP6208(config-if-4)# dhcp-gateway-list 1
```

Syntax: dhcp-gateway-list <num> <ip-addr>

Possible values: N/A

Default value: N/A

enable password

Three levels of passwords can be assigned to provide a range of access point for various users within the network.

The three levels are:

- Superuser: This user has unlimited access to all levels of the CLI. This level is generally reserved for system administration. The super user is also the only user that can assign a password access level to another user.
- Configure Port: This user has the ability to configure interface parameters only. The user can also use the show commands.
- Read only: A user with this password level is able to use only the show commands. No configuration is allowed with this access type.

EXAMPLE:

```
HP9300(config)# enable super-user-password Dan
HP9300(config)# enable read-only-password Matt
HP9300(config)# enable port-config-password Alex
```

Syntax: enable super-user-password | read-only-password | port-config-password <text>

Possible values: Up to 32 alphanumeric characters can be assigned in the text field.

Default value: No system default

enable skip-page-display

Removes the stop page display characteristic for the **write terminal** command. For example, by default, when you enter the command **write terminal**, the full configuration file displayed will generally involve more than a single page display. You are prompted to press the Return key to view the next page of information. When this command is enabled, this page-by-page prompting will be removed and the entire display will roll on the screen until the end is reached.

To re-enable the stop page display characteristic, enter the **no enable skip-page-display**.

EXAMPLE:

To remove the page-by-page display of configuration information, enter the following:

```
HP9300(config)# enable skip-page-display
```

Syntax: enable skip-page-display

Possible values: N/A

Default value: Disabled

enable snmp config-radius

Enables users of SNMP management applications to configure RADIUS authentication parameters on the HP device.

EXAMPLE:

To enable SNMP management application users to configure RADIUS authentication parameters on the HP device, enter the following:

```
HP9300(config)# enable snmp config-radius
```

Syntax: enable snmp config-radius

Possible values: N/A

Default value: Disabled

enable snmp config-tacacs

Enables users of SNMP management applications to configure TACACS/TACACS+ authentication parameters on the HP device.

EXAMPLE:

To enable SNMP management application users to configure TACACS/TACACS+ authentication parameters on the HP device, enter the following:

```
HP9300(config)# enable snmp config-tacacs
```

Syntax: enable snmp config-tacacs

Possible values: N/A

Default value: Disabled

enable telnet authentication

Allows you to use local access control, a RADIUS server, or a TACACS/TACACS+ server to authenticate telnet access to the device.

EXAMPLE:

```
HP9300(config)# enable telnet authentication
```

Syntax: [no] enable telnet authentication

Possible values: N/A

Default value: Disabled

enable telnet password

Allows you to assign a password for Telnet session access. To close a Telnet session, enter **logout**.

EXAMPLE:

```
HP9300(config)# enable telnet password secretsalso
```

Syntax: enable telnet password <text>

Possible values: Up to 32 alphanumeric characters can be assigned as the password.

Default value: No system default.

end

Moves activity to the privileged EXEC level from any level of the CLI, with the exception of the user level.

EXAMPLE:

To move to the privileged level, enter the following from any level of the CLI.

```
HP9300(config)# end
HP9300#
```

Syntax: end

Possible values: N/A

Default value: N/A

exit

Moves activity up one level from the current level. In this case, activity will be moved to the privileged level.

EXAMPLE:

To move from the global level, back to the privileged level, enter the following:

```
HP9300(config)# exit
HP9300#
```

Syntax: exit

Possible values: N/A

Default value: N/A

fast port-span

Configures the Fast Port Span feature, which allows faster STP convergence on ports that are attached to end stations.

EXAMPLE:

To enable Fast Port Span:

```
HP9300(config)# fast port-span
```

EXAMPLE:

To exclude a port from Fast Port Span, while leaving Fast Port Span enabled globally:

```
HP9300(config)# fast port-span exclude ethernet 1/1
```

Syntax: [no] fast port-span [exclude ethernet <portnum> [ethernet <portnum>… | to <portnum>]

Possible values: Valid port numbers

Default value: Enabled

fast uplink-span

Configures the Fast Uplink Span feature, which reduces the convergence time for uplink ports to another device to just four seconds (two seconds for listening and two seconds for learning).

EXAMPLE:

To configure a group of ports for Fast Uplink Span, enter the following commands:

```
HP9300(config)# fast uplink-span ethernet 4/1 to 4/4
```

Syntax: [no] fast uplink-span [ethernet <portnum> [ethernet <portnum>… | to <portnum>]

Possible values: Ports that have redundant uplinks on a wiring closet switch.

Default value: Disabled

flow-control

Allows you to turn flow control (802.3x) for full-duplex ports on or off (no). By default, flow control is on. To turn the feature off, enter the command **no flow-control**.

EXAMPLE:

```
HP9300(config)# no flow-control
```

To turn the feature back on later, enter the following command:

```
HP9300(config)# flow-control
```

Syntax: [no] flow-control

Possible values: N/A

Default value: on

gig-default

Changes the default negotiation mode for Gigabit ports. You can configure the default Gigabit negotiation mode to be one of the following:

- Negotiate-full-auto – The port first tries to perform a handshake with the other port to exchange capability information. If the other port does not respond to the handshake attempt, the port uses the manually configured configuration information (or the defaults if an administrator has not set the information). This is the default.
- Auto-Gigabit – The port tries to perform a handshake with the other port to exchange capability information.
- Negotiation-off – The port does not try to perform a handshake. Instead, the port uses configuration information manually configured by an administrator.

See the “Configuring Basic Features” chapter of the *Installation and Getting Started Guide* for more information.

EXAMPLE:

To change the mode globally to negotiation-off, enter the following command:

```
HP9300(config)# gig-default neg-off
```

To override the global default on an individual Gigabit port, see “gig-default” on page 7-4.

Syntax: gig-default neg-full-auto | auto-gig | neg-off

Possible values: see above

Default value: neg-full-auto

hostname

Changes the host name to more easily identify Fixed-port devices within the network.

EXAMPLE:

To change the hostname of an HP 6308M-SX to “Router1” from the default, “HP6308”, enter the following:

```
HP6308(config)# hostname Router1
Router1(config)#
```

Syntax: hostname <text>

Possible values: Up to 32 alphanumeric characters can be assigned to hostname text string.

Default value: HP6308 or HP6208

interface

Accesses the interface CONFIG level of the CLI. You can define a physical interface, loopback interface, or virtual interface (ve) at the Interface level.

By default, you can add up to 24 IP addresses to a physical, virtual, or loopback interface.

You can configure up to 64 virtual interfaces on a Fixed-port device routing switch and up to 255 virtual interfaces on a routing switch.

You can configure up to eight loopback interfaces on a routing switch.

EXAMPLE:

To change the configuration for port 1 on a Fixed-port device, enter the following:

```
HP6208(config)# inter e 1
HP6208(config-if-1)#
```

NOTE: To change the port for a Chassis device, you also need to enter the slot number of the module on which the port resides.

Syntax: interface ethernet <portnum> [to <portnum>]

Syntax: interface loopback <num>

Syntax: interface ve <num>

EXAMPLE:

To add a virtual interface to a routing switch, enter the following. Use commands at the Virtual Interface level (vif) to configure the interface.

```
HP9300(config)# inter ve 1
HP9300(config-vif-1)#
```

Syntax: interface ve <num>

Possible values: 1 – 255

Default value: N/A

EXAMPLE:

To add a loopback interface to a routing switch, enter the following:

```
HP9300(config)# int loopback 1
HP9300(config-lbif-1)# ip address 10.0.0.1/24
```

Syntax: interface loopback <num>

Possible values: 1 – 8

Default value: N/A

ip access-list

Configures a named IP ACL.

You can use this command to configure a standard or extended IP ACL.

The commands for configuring named ACL entries are different from the commands for configuring numbered ACL entries. The command to configure a numbered ACL is **access-list**. The command for configuring a named ACL is **ip access-list**. In addition, when you configure a numbered ACL entry, you specify all the command parameters on the same command. When you configure a named ACL, you specify the ACL type (standard or extended) and the ACL number with one command, which places you in the configuration level for that ACL. Once you enter the configuration level for the ACL, the command syntax is the same as the syntax for numbered ACLs.

EXAMPLE:

To configure a named standard ACL entry, enter commands such as the following.

```
HP9300(config)# ip access-list standard Net1
HP9300(config-std-nacl)# deny host 209.157.22.26 logl
HP9300(config-std-nacl)# deny 209.157.29.12 log
HP9300(config-std-nacl)# deny host IPHost1 log
HP9300(config-std-nacl)# permit any
HP9300(config-std-nacl)# exit
HP9300(config)# int eth 1/1
HP9300(config-if-1/1)# ip access-group Net1 out
```

The commands in this example configure a standard ACL named “Net1”. The entries in this ACL deny packets from three source IP addresses from being forwarded on port 1/1. Since the implicit action for an ACL is “deny”, the last ACL entry in this ACL permits all packets that are not explicitly denied by the first three ACL entries. For an example of how to configure the same entries in a numbered ACL, see the “Configuring Standard ACLs“ section of the “Using Access Control Lists (ACLs)” chapter in the *Advanced Configuration and Management Guide*.

Notice that the command prompt changes after you enter the ACL type and name. The “std” in the command prompt indicates that you are configuring entries for a standard ACL. For an extended ACL, this part of the command prompt is “ext“. The “nacl” indicates that are configuring a named ACL.

Syntax: ip access-list extended | standard <string> | <num>

The **extended | standard** parameter indicates the ACL type.

The<string> parameter is the ACL name. You can specify a string of up to 256 alphanumeric characters. You can use blanks in the ACL name if you enclose the name in quotation marks (for example, “ACL for Net1”). The <num> parameter allows you to specify an ACL number if you prefer. If you specify a number, you can specify from 1 – 99 for standard ACLs or 100 – 199 for extended ACLs.

NOTE: For convenience, the software allows you to configure numbered ACLs using the syntax for named ACLs. The software also still supports the older syntax for numbered ACLs. Although the software allows both methods for configuring numbered ACLs, numbered ACLs are always formatted in the startup-config and running-config files in using the older syntax, as follows.

```
access-list 1 deny host 209.157.22.26 log
access-list 1 deny 209.157.22.0 0.0.0.255 log
access-list 1 permit any
access-list 101 deny tcp any any eq http log
```

The options at the ACL configuration level and the syntax for the **ip access-group** command are the same for numbered and named ACLs. See “access-list (standard)” on page 6-2.

EXAMPLE:

To configure a named extended ACL entry, enter commands such as the following.

```
HP9300(config)# ip access-list extended “block Telnet”
HP9300(config-ext-nacl)# deny tcp host 209.157.22.26 any eq telnet log
HP9300(config-ext-nacl)# permit ip any any
HP9300(config-ext-nacl)# exit
HP9300(config)# int eth 1/1
HP9300(config-if-1/1)# ip access-group “block Telnet” in
```

The options at the ACL configuration level and the syntax for the **ip access-group** command are the same for numbered and named ACLs. See “access-list (extended)” on page 6-3.

Possible values: see above

Default value: N/A

ip access-policy

Configures permit and deny policies and Layer 4 QoS policies on switches and routing switches. See the “Policies and Filters” appendix of the *Advanced Configuration and Management Guide* for more information.

NOTE: Access policies on routing switches can permit or deny packets (filter) or allocate packets to specific QoS levels. Access policies on switches can only allocate traffic to specific QoS levels.

NOTE: After you configure an IP access policy, you need to apply it to specific ports using the **ip access-policy-group** command at the Interface level of the CLI. See “ip access-policy-group” on page 7-5.

Permit and Deny Policies

IP access policies are rules that determine whether the device forwards or drops IP packets. You create an IP access policy by defining an IP filter, then applying it to an interface. The filter consists of source and destination IP information and the action to take when a packet matches the values in the filter. You can configure an IP filter to permit (forward) or deny (drop) the packet.

NOTE: You can configure permit and deny IP access policies only on routing switches, not on switches. On switches, the **ip access-policy** command configures Layer 4 QoS.

You can apply an IP filter to inbound or outbound packets. When you apply the filter to an interface, you specify whether the filter applies to inbound packets or outbound packets. Thus, you can use the same filter on multiple interfaces and specify the filter direction independently on each interface.

EXAMPLE:

To configure an IP access policy to explicitly permit HTTP traffic (TCP port 80) from IP address 10.0.0.1 on port 1/2, enter the following commands:

```
HP9300(config)# ip access-policy 2 permit 10.0.0.1 255.0.0.0 tcp eq 80
HP9300(config)# int e 1/2
HP9300(config-if-1/2)# ip access-policy-group in 2
```

Here is the syntax for Chassis devices.

Syntax: ip access-policy <num> deny | permit <ip-addr> <ip-mask> | any <ip-addr> <ip-mask> | any icmp | igmp | igrp | ospf | tcp | udp | <num> [<operator> [<tcp/udp-port-num>]] [log]

ip access-policy-group in | out <policy-list>

Here is the syntax for Fixed-port devices.

Syntax: ip access-policy <num> deny | permit <ip-addr> <mask> | any <ip-addr> <mask> | any tcp | udp [<operator> [<tcp/udp-port-num>]] [log]

ip access-policy-group in | out <policy-list>

The <num> parameter is the policy number.

The **deny | permit** parameter specifies the action the router takes if a packet matches the policy.

- If you specify deny, the router drops the packet.
- If you specify permit, the router forwards the packet.

The <ip-addr> <ip-mask> **| any** <ip-addr> <ip-mask> **| any** parameters specify the source and destination IP addresses. If you specify a particular IP address, you also need to specify the mask for that address. If you specify **any** to apply the policy to all source or destination addresses, you do not need to specify **any** again for the mask. Make sure you specify a separate address and mask or **any** for the source and destination address.

The **icmp | igmp | igrp | ospf | tcp | udp |** <num> parameter specifies the Layer 4 port to which you are applying the policy. If you specify **tcp** or **udp**, you also can use the optional <operator> and <tcp/udp-port-num> parameters to fine-tune the policy to apply to specific TCP or UDP ports.

The <operator> parameter applies only if you use the **tcp** or **udp** parameter above. Use the <operator> parameter to specify the comparison condition for the specific TCP or UDP ports. For example, if you are configuring QoS for HTTP, specify **tcp eq http**. You can enter one of the following operators:

- **eq** – The policy applies to the TCP or UDP port name or number you enter after **eq**.
- **gt** – The policy applies to TCP or UDP port numbers greater than the port number or the numeric equivalent of the port name you enter after **gt**.
- **lt** – The policy applies to TCP or UDP port numbers that are less than the port number or the numeric equivalent of the port name you enter after **lt**.
- **neq** – The policy applies to all TCP or UDP port numbers except the port number or port name you enter after **neq**.
- **range** – The policy applies to all TCP or UDP port numbers that are between the first TCP or UDP port name or number and the second one you enter following the range parameter. The range includes the port names or numbers you enter. For example, to apply the policy to all ports between and including 23 (Telnet) and 53 (DNS), enter the following: **range 23 53**. The first port number in the range must be lower than the last number in the range.

- **established** – This operator applies only to TCP packets. If you use this operator, the policy applies to TCP packets that have the ACK (Acknowledgment) or RST (Reset) bits set on (set to "1") in the Control Bits field of the TCP packet header. Thus, the policy applies only to established TCP sessions, not to new sessions. See Section 3.1, "Header Format", in RFC 793 for information about this field.

The **log** parameter applies only to deny policies. This parameter generates a Syslog entry for packets that are denied by the policy. See Example 4 in “show logging” on page 20-35.

Layer 4 Policies

EXAMPLE:

To assign a priority of 4 to all HTTP traffic on port 3/12, enter the following:

```
HP9300(config)# ip access-policy 1 priority 4 any any tcp eq http
HP9300(config)# int e 3/12
HP9300(config-if-3/12)# ip access-policy-group out 1
```

Syntax: ip access-policy <num> priority <0-7> <ip-addr> <ip-mask> | any <ip-addr> <ip-mask> | any tcp | udp [<operator> [<tcp/udp-port-num>]]

ip access-policy-group in | out <policy-list>

The <num> parameter is the policy number.

The **priority** <0-7> parameter specifies the QoS priority level. The default is 0 (normal priority). The highest priority is 7.

The <ip-addr> <ip-mask> **| any** <ip-addr> <ip-mask> **| any** parameters specify the source and destination IP addresses. If you specify a particular IP address, you also need to specify the mask for that address. If you specify **any** to apply the policy to all source or destination addresses, you do not need to specify **any** again for the mask. Make sure you specify a separate address and mask or **any** for the source and destination address.

The **icmp | igmp | igrp | ospf | tcp | udp |** <num> parameter specifies the Layer 4 port to which you are applying the policy. If you specify **tcp** or **udp**, you also can use the optional <operator> and <tcp/udp-port-num> parameters to fine-tune the policy to apply to specific TCP or UDP ports.

The <operator> parameter applies only if you use the **tcp** or **udp** parameter above. Use the <operator> parameter to specify the comparison condition for the specific TCP or UDP ports. For example, if you are configuring QoS for HTTP, specify **tcp eq http**. You can enter one of the following operators:

- **eq** – The policy applies to the TCP or UDP port name or number you enter after **eq**.
- **gt** – The policy applies to TCP or UDP port numbers greater than the port number or the numeric equivalent of the port name you enter after **gt**.
- **lt** – The policy applies to TCP or UDP port numbers that are less than the port number or the numeric equivalent of the port name you enter after **lt**.
- **neq** – The policy applies to all TCP or UDP port numbers except the port number or port name you enter after **neq**.
- **range** – The policy applies to all TCP or UDP port numbers that are between the first TCP or UDP port name or number and the second one you enter following the range parameter. The range includes the port names or numbers you enter. For example, to apply the policy to all ports between and including 23 (Telnet) and 53 (DNS), enter the following: **range 23 53**. The first port number in the range must be lower than the last number in the range.
- **established** – This operator applies only to TCP packets. If you use this operator, the QoS policy applies to TCP packets that have the ACK (Acknowledgment) or RST (Reset) bits set on (set to "1") in the Control Bits field of the TCP packet header. Thus, the policy applies only to established TCP sessions, not to new sessions. See Section 3.1, "Header Format", in RFC 793 for information about this field.

ip address

Assigns an IP address and network mask to a switch to support Telnet and SNMP management.

EXAMPLE:

```
HP6208(config)# ip address 192.22.3.44 255.255.255.0
```

```
HP6208(config)# ip address 192.22.3.44/24
```

Syntax: ip address <ip-addr> <ip-mask>

or

Syntax: ip address <ip-addr>/<mask-bits>

Possible values: N/A

Default value: N/A

ip arp-age

Defines how long an ARP entry will be resident in the ARP cache before it is aged out.

EXAMPLE:

```
HP9300(config)# ip arp-age 20
```

Syntax: ip arp-age <minutes>

Possible values: 0 – 240 minutes

Default value: 10 minutes

ip as-path

Configures an AS-path ACL. You can use AS-path ACLs to permit or deny routes based on their AS path information.

EXAMPLE:

To configure an AS-path list that uses ACL 1, enter a command such as the following:

```
HP9300(config)# ip as-path access-list 1 permit 100
HP9300(config)# router bgp
HP9300(config-bgp-router)# neighbor 10.10.10.1 filter-list 1 in
```

The **ip as-path** command configures an AS-path ACL that permits routes containing AS number 100 in their AS paths. The **neighbor** command then applies the AS-path ACL to advertisements and updates received from neighbor 10.10.10.1. In this example, the only routes the routing switch permits from neighbor 10.10.10.1 are those whose AS-paths contain AS-path number 100.

Syntax: ip as-path access-list <num> [seq <seq-value>] deny | permit <as-regular-expression>

The <num> parameter specifies the ACL number and can be from 1 – 199.

The **seq** <seq-value> parameter is optional and specifies the AS-path list's sequence number. You can configure up to 199 entries in an AS-path list. If you do not specify a sequence number, the software numbers them in increments of 5, beginning with number 5. The software interprets the entries in an AS-path list in numerical order, beginning with the lowest sequence number.

The **deny | permit** parameter specifies the action the software takes if a route's AS-path list matches a match statement in this ACL. To configure the AS-path match statements, use the **match as-path** command. See "match" on page 15-1.

The <AS-regular-expression> parameter specifies the AS path information you want to permit or deny to routes that match any of the match statements within the ACL. You can enter a specific AS number or use a regular expression. For the regular expression syntax, see the "Configuring BGP4" chapter of the *Advanced Configuration and Management Guide*.

The **neighbor** command uses the **filter-list** parameter to apply the AS-path ACL to the neighbor. See "neighbor" on page 14-9.

Possible values: see above

Default value: N/A

ip community-list

Configures a community ACL. You can use community ACLs to permit or deny routes based on their communities.

EXAMPLE:

To configure community ACL 1, enter a command such as the following:

```
HP9300(config)# ip community-list 1 permit 123:2
```

This command configures a community ACL that permits routes that contain community 123:2.

NOTE: See “match” on page 15-1 for information about how to use a community list as a match condition in a route map.

Syntax: ip community-list <num> [seq <seq-value>] deny | permit <community-num>

The <num> parameter specifies the ACL number and can be from 1 – 199.

The **seq** <seq-value> parameter is optional and specifies the community list’s sequence number. You can configure up to 199 entries in a community list. If you do not specify a sequence number, the software numbers them in increments of 5, beginning with number 5. The software interprets the entries in a community list in numerical order, beginning with the lowest sequence number.

The **deny | permit** parameter specifies the action the software takes if a route’s community list matches a match statement in this ACL. To configure the community-list match statements, use the **match community-list** command. See “match” on page 15-1.

The <community-num> parameter specifies the community type or community number. This parameter can have the following values:

- <num>**:**<num> – A specific community number
- **internet** – The Internet community
- **no-export** – The community of sub-ASs within a confederation. Routes with this community can be exported to other sub-ASs within the same confederation but cannot be exported outside the confederation to other ASs or otherwise sent to EBGP neighbors.
- **local-as** – The local sub-AS within the confederation. Routes with this community can be advertised only within the local subAS.
- **no-advertise** – Routes with this community cannot be advertised to any other BGP4 routers at all.

Possible values: see above

Default value: N/A

ip default-gateway

Assigns an IP address and mask to a switch to support Telnet and SNMP management.

This command is not available on HP routers.

EXAMPLE:

```
HP6208(config)# ip default-gateway 192.22.33.100
```

Syntax: ip default-gateway <ip-addr>

Possible values: N/A

Default value: N/A

ip default-network

Configures a default network route, use one of the following methods. You can configure up to four default network routes.

EXAMPLE:

To configure a default network route, enter commands such as the following:

```
HP9300(config)# ip default-network 209.157.22.0
HP9300(config)# write mem
```

Syntax: ip default-network <ip-addr>

The <ip-addr> parameter specifies the network address.

To verify that the route is in the route table, enter the following command at any level of the CLI:

```
HP9300(config)# show ip route

Total number of IP routes: 2
Start index: 1  B:BGP D:Connected  R:RIP  S:Static  O:OSPF *:Candidate default
      Destination       NetMask           Gateway           Port   Cost   Type
1     209.157.20.0      255.255.255.0     0.0.0.0           lb1    1      D
2     209.157.22.0      255.255.255.0     0.0.0.0           4/11   1      *D
```

This example shows two routes. Both of the routes are directly attached, as indicated in the Type column. However, one of the routes is shown as type “*D”, with an asterisk (*). The asterisk indicates that this route is a candidate default network route.

Possible values: valid IP network address

Default value: N/A

ip directed-broadcast

Enables or disables forwarding of directed IP broadcasts on a routing switch.

EXAMPLE:

```
HP9300(config)# ip directed-broadcast
```

Syntax: [no] ip directed-broadcast

Possible values: N/A

Default value: disabled

ip dns domain-name

Defines a domain name for a range of addresses on the HP switch or router. This eliminates the need to type in the domain name. It will automatically be appended to the hostname.

EXAMPLE:

```
HP9300(config)# ip dns domain-name newyork.com
```

Syntax: ip dns domain-name

Possible values: N/A

Default value: N/A

ip dns server-address

Up to four DNS servers can be defined for each DNS entry. The first entry serves as the primary default address (207.95.6.199). If a query to the primary address fails to be resolved after three attempts, the next gateway address will be queried for three times as well. This process will continue for each defined gateway address until a query is resolved. The order in which the default gateway addresses are polled is tied to the order in which they are entered when initially defined as shown in the example.

EXAMPLE:

```
HP9300(config)# ip dns server-address 207.95.6.199 205.96.7.1 5 208.95.7.25
201.98.7.15
```

Syntax: ip dns server-address <ip-addr> [<ip-addr>] [<ip-addr>] [<ip-addr>]

Possible values: Up to four IP addresses

Default value: N/A

ip dont-use-acl

Disables all packet-forwarding IP ACLs (those associated with specific ports) and also prevents you from associating an IP ACL with a port. However, the command does not remove existing IP ACLs from the startup-config file. In addition, the command does not affect IP ACLs used for controlling management access to the device.

NOTE: A routing switch cannot actively use both IP access policies and IP ACLs for filtering IP traffic. When you boot a routing switch with software release 06.x or higher, the software checks the device's startup-config file for **ip access-policy-group** commands, which associate IP access policies with ports. If the software finds an **ip access-policy-group** command in the file, the software disables all packet-forwarding IP ACLs (those associated with specific ports) and also prevents you from applying an IP ACL to a port.

The next time you save the startup-config file, the software adds the **ip dont-use-acl** command near the top of the file, underneath the **ver** (software version) statement.

EXAMPLE:

Disabling ACL Mode

If the ACL mode is enabled, a message is displayed when you try to apply an IP access policy to a port, as shown in the following CLI example:

```
HP9300(config-if-e1000-1/1)# ip access-policy-group 1 in
Must disable ACL mode first by using ip dont-use-acl command, write memory and
reload
```

To disable the ACL mode, enter the following commands:

```
HP9300(config-if-e1000-1/1)# exit
HP9300(config)# ip dont-use-acl
HP9300(config)# write mem
HP9300(config)# end
HP9300# reload
```

EXAMPLE:

Enabling ACL Mode

If you try to apply an IP ACL to a port when the ACL mode is disabled (when the **ip dont-use-acl** command is in effect), a message is displayed, as shown in the following CLI example:

```
HP9300(config-if-e1000-1/1)# ip access-group 1 out
Must enable ACL mode first by using no ip dont-use-acl command and removing all ip
access-policy-group commands from interfaces, write memory and reload
```

As the message states, if you want to use IP ACLs, you must first enable the ACL mode. To do so, use either of the following methods.

To enable the ACL mode, enter the following commands:

```
HP9300(config-if-e1000-1/1)# exit
HP9300(config)# no ip dont-use-acl
```

```
HP9300(config)# write mem
HP9300(config)# end
HP9300# reload
```

The **write mem** command removes the **ip dont-use-acl** command from the startup-config file. The **reload** command reloads the software. When the software finishes loading, you can apply IP ACLs to ports.

The commands that configure the IP access policies and apply them to ports remain in the startup-config file in case you want to use them again, but they are disabled. If you later decide you want to use the IP access policies again instead of IP ACLs, you must disable the IP ACL mode again. See Example 1 above.

Syntax: [no] ip dont-use-acl

Possible values: N/A

Default value: see above

ip forward-protocol

This command is used in conjunction with the UDP helper feature to define the type of application traffic (port number socket) that is being forwarded to the server.

This command is not supported on HP switches.

EXAMPLE:

```
HP9300(config)# ip-forward-protocol udp snmp-trap
```

Syntax: ip forward-protocol udp <udp-application-name> | <udp-application-num>

Possible values:

number	echo	snmp-trap
bootpc	mobile-ip	tacacs
bootps	netbios-dgm	talk
discard	netbios-ns	
dnsix	ntp	
tftp	snmp	

In addition, you can specify any UDP application by using the application's UDP port number.

Default value: By default, when an IP helper address is configured on an interface, UDP broadcast forwarding is enabled for the following UDP packet types: bootps, domain, tftp, time, netbios-dgm, netbios-ns and tacacs.

ip igmp group-membership-time

Defines how long a group will remain on an interface in the absence of a group report, if DVMRP is enabled on the router.

NOTE: You must enter the **ip multicast-routing** command before entering this command. Otherwise, the command does not take effect and the software uses the default value.

EXAMPLE:

```
HP9300(config)# ip igmp group-membership-time 240
```

Syntax: ip igmp group-membership-time <value>

Possible values: 1 – 7200 seconds

Default value: 140 seconds

ip igmp max-response-time

Defines how many seconds the routing switch will wait for an IGMP response from an interface before concluding that the group member on that interface is down and removing the interface from the group.

NOTE: You must enter the **ip multicast-routing** command before entering this command. Otherwise, the command does not take effect and the software uses the default value.

EXAMPLE:

```
HP9300(config)# ip igmp max-response-time 5
```

Syntax: ip igmp max-response-time <value>

Possible values: 1 – 10 seconds

Default value: 10 seconds

ip igmp query-interval

Defines how often the router will query an interface for group membership.

NOTE: You must enter the **ip multicast-routing** command before entering this command. Otherwise, the command does not take effect and the software uses the default value.

EXAMPLE:

```
HP9300(config)# ip igmp query 120
```

Syntax: ip igmp query-interval <value>

Possible values: 1 – 3600 seconds

Default value: 60 seconds

ip irdp

Enables a router to advertise its network IP addresses to the network. The router will also answer queries. IRDP stands for ICMP Router Discovery Protocol (IRDP).

EXAMPLE:

```
HP9300(config)# ip irdp
```

Syntax: [no] ip irdp

Possible values: n/a

Default value: enabled

ip load-sharing

Allows traffic being sent from one router to another to be sent across multiple paths of equal cost for faster transmission when using OSPF or BGP4 routing. OSPF or BGP4 routing must be enabled on the router for this command to operate. IP load sharing is enabled by default.

See the “Configuring OSPF” chapter of the *Advanced Configuration and Management Guide* for more information about this feature.

EXAMPLE:

```
HP9300(config)# ip load-sharing 6
```

Syntax: ip load-sharing [<num>]

The <num> parameter specifies the number of equal paths across which the routing switch will load share traffic to a given destination.

Possible values: 2 – 8

Default value: 4

ip mroute

Configures a static multicast route. If you configure more than one static multicast route, the routing switch always uses the most specific route that matches a multicast source address. Thus, if you want to configure a multicast static route for a specific multicast source and also configure another multicast static route for all other sources, you can configure two static routes.

EXAMPLE:

```
HP9300(config)# ip mroute 1 207.95.10.0/24 interface ethernet 1/2 distance 1
```

Syntax: mroute <routenum> <ip-addr> interface ethernet <portnum> | ve <num> [distance <num>]

Or

Syntax: mroute <routenum> <ip-addr> rpf_address <rpf-num>

Possible values: The <ip-addr> parameter specifies the PIM source for the route.

NOTE: In IP multicasting, a route is handled in terms of its source, rather than its destination.

You can use the **ethernet** <portnum> parameter to specify a physical port or the **ve** <num> parameter to specify a virtual interface.

The **distance** <num> parameter sets the administrative distance for the route. When comparing multiple paths for a route, the routing switch prefers the path with the lower administrative distance.

NOTE: Regardless of the administrative distances, the routing switch always prefers directly connected routes over other routes.

The **rpf_address** <rpf-num> parameter specifies an RPF number.

Default value: N/A

ip multicast

Enables IP Multicast Traffic Reduction on an HP switch. A switch can operate in either an active or passive IP multicast mode. You must save changes to flash and reset (reload) the switch for the configuration changes to become active. For more details on this feature, see the “Installation” chapter of the *Installation and Getting Started Guide*.

- If configured to be active, the switch will actively send out host queries to identify IP Multicast groups on the network and insert this information in the IGMP packet. Routers in the network generally handle this operation.
- If configured to be passive, the switch will only identify the packet as an IGMP packet and forward it accordingly.

EXAMPLE:

```
HP6208(config)# ip multicast passive

HP6208(config)# write memory

HP6208(config)# end

HP6208# reload
```

Syntax: ip multicast active | passive

Possible values: Active or passive

Default value: Disabled

ip multicast-routing

Allows you to change the following global IP Multicast parameters:

- IGMP query interval
- IGMP group membership time
- IGMP maximum response time

NOTE: You must enter the **ip multicast-routing** command before changing these parameters. Otherwise, the changes do not take effect and the software uses the default values.

EXAMPLE:

```
HP9300(config)# ip multicast-routing
```

Syntax: [no] ip multicast-routing

Possible values: N/A

Default value: Disabled

ip prefix-list

Configures an IP prefix list. You can configure a range of IP prefixes for routes you want to send to or receive from individual neighbors.

EXAMPLE:

To configure an IP prefix list and apply it to a neighbor, enter commands such as the following:

```
HP9300(config)# ip prefix-list Routesfor20 permit 20.20.0.0/24
HP9300(config-bgp-router)# neighbor 10.10.10.1 prefix-list Routesfor20 out
```

These commands configure an IP prefix list named Routesfor20, which permits routes to network 20.20.0.0. The **neighbor** command configures the routing switch to use IP prefix list Routesfor20 to determine which routes to send to neighbor 10.10.10.1. The routing switch sends routes that go to 20.20.x.x to neighbor 10.10.10.1 because the IP prefix list explicitly permits these routes to be sent to the neighbor.

Syntax: ip prefix-list <name> [seq <seq-value>] [description <string>] deny | permit <network-addr>/<mask-bits> [ge <ge-value>] [le <le-value>]

The <name> parameter specifies the prefix list name. You use this name when applying the prefix list to a neighbor.

The **description** <string> parameter is a text string describing the prefix list.

The **seq** <seq-value> parameter is optional and specifies the IP prefix list's sequence number. You can configure up to 100 prefix list entries. If you do not specify a sequence number, the software numbers them in increments of 5, beginning with prefix list entry 5. The software interprets the prefix list entries in numerical order, beginning with the lowest sequence number.

The **deny | permit** parameter specifies the action the software takes if a neighbor's route is in this prefix list.

The prefix-list matches only on this network unless you use the **ge** <ge-value> or **le** <le-value> parameters. (See below.)

The <network-addr>/<mask-bits> parameter specifies the network number and the number of bits in the network mask.

The **ge** <ge-value> parameter specifies a range of prefixes more specific than the range specified by <network-addr>/<mask-bits> that still match the prefix list. The <ge-value> specifies the minimum number of mask bits in the network mask. For example, if you add **ge 24** to the command above, the prefix list matches on all network numbers that are equal to or more specific than 20.20.0.0. Thus 20.20.1.0 and higher also match the prefix list.

The **le** <ge-value> parameter specifies a range of prefixes less specific than the range specified by <network-addr>/<mask-bits> that still match the prefix list. The <le-value> specifies the maximum number of bits

in the mask. For example, if you add **le 16** to the command above, the prefix list matches on 20.20.x.x and on all other 20.x.x.x networks.

If you do not specify **ge** <ge-value> or **le** <le-value>, the prefix list matches only on the exact network prefix you specify with the <network-addr>/<mask-bits> parameter.

For the syntax of the **neighbor** command shown in the example above, see “neighbor” on page 14-9.

Possible values: see above

Default value: N/A

ip proxy-arp

Allows a router to act as a proxy for devices on its interfaces when responding to ARP requests.

EXAMPLE:

```
HP9300(config)# ip proxy
```

Syntax: ip proxy-arp

Possible values: On or off

Default value: On

ip rarp

Enables Reverse Addressing Resolution Protocol (RARP) and allows the router to assign IP addresses for hosts based on their MAC addresses. A router will check the RARP table for an IP match to a MAC address sent from a host. If the table contains an entry for the MAC address, the router will answer back with the IP address.

EXAMPLE:

```
HP9300(config)# ip rarp
```

Syntax: ip rarp

Possible values: N/A

Default value: N/A

ip route

Allows you to configure static IP routes for an HP router.

EXAMPLE:

```
HP9300(config)# ip route 192.128.2.69 255.255.255.0 209.157.22.1
```

Syntax: [no] ip route <ip-addr> <mask> <next-hop-ip-addr> | null0 [<metric>] [distance <num>]

or

Syntax: [no] ip route <ip-addr>/<mask-bits> <next-hop-ip-addr> | null0 [<metric>] [distance <num>]

The <metric> parameter can be a number from 1 – 16. The default is 1.

NOTE: If you specify 16, RIP considers the metric to be infinite and thus also considers the route to be unreachable.

The <dest-ip-addr> and <dest-mask> parameters specify the route’s destination. You can enter multiple static routes for the same destination for load balancing or redundancy. See the “Defining Static IP Routes” section in the “Configuring IP and IP/RIP” chapter in the *Advanced Configuration and Management Guide*.

The **distance** <num> parameter specifies the administrative distance of the route. When comparing otherwise equal routes to a destination, the routing switch prefers lower administrative distances over higher ones, so make sure you use a low value for your default route. The default is 1.

NOTE: You can also assign the default router as the destination by entering 0.0.0.0 0.0.0.0.

Default value: metric 1, distance 1

NOTE: The router will replace the static route if the router receives a route with a lower administrative distance. See the “Configuring BGP4” chapter of the *Advanced Configuration and Management Guide* for a list of the default administrative distances for all types of routes.

ip router-id

Assigns a router ID to an HP routing switch. OSPF and BGP4 use router IDs to identify routers. A routing switch can have one router ID, which is used by both OSPF and BGP4 if both are enabled.

Router IDs are in IP address format (for example, 1.1.1.1). The default router ID is the IP address configured on the lowest numbered loopback interface configured on the routing switch. If the device does not have any loopback interfaces, the default router ID is the lowest numbered IP interface configured on the device. This ensures that the router ID on each router is unique even if you use the default value.

EXAMPLE:

```
HP9300(config)# ip router-id 1.1.1.1
```

Syntax: ip router-id <ip-addr>

Possible values: N/A

Default value: the numerically lowest IP address configured on the routing switch

ip show-subnet-length

Changes display of network mask information from class-based notation (xxx.xxx.xxx.xxx) to Classless Interdomain Routing (CIDR) notation. By default, HP devices display network mask information in class-based notation.

EXAMPLE:

```
HP9300(config)# ip show-subnet-length
```

Syntax: [no] ip show-subnet-length

Possible values: N/A

Default value: Disabled

ip source-route

Disables or re-enables forwarding of IP source-routed packets.

EXAMPLE:

To disable forwarding of IP source-routed packets, enter the following command:

```
HP9300(config)# no ip source-route
```

Syntax: [no] ip source-route

To re-enable forwarding of source-routed packets, enter the following command:

```
HP9300(config)# ip source-route
```

Possible values: N/A

Default value: Disabled

ip ttl

Sets the maximum time that a packet will live on the network.

This command applies both to routing switches and to switches.

EXAMPLE:

```
HP9300(config)# ip ttl 25
HP9300(config)# exit
HP9300# write mem
```

Syntax: ip ttl <hops>

Possible values: 1 – 255 hops

Default value: 64 hops

ipx forward-filter

Defines forward filters for IPX routes.

IPX must be enabled and a network number and frame type defined for each IPX interface, for this command to be operational.

EXAMPLE:

```
HP9300(config)# ipx forward-filter 2 permit 1110005 451 11101050 120 any
```

Syntax: ipx forward-filter <index> permit | deny <source-network-number> | any <source-node-number> | any <destination-network-number> | any <destination-node-number> | any <destination-socket-number> | any

Possible values: up to 32 forward filters

Default value: N/A

ipx gns-round-robin

Configures the routing switch to use round-robin to rotate among servers of a given service type when responding to GNS requests, instead of the default behavior of responding with the most recently learned server supporting the requested service.

EXAMPLE:

To enable the routing switch to use round-robin to select servers for replies to GNS requests:

```
HP9300(config)# ipx gns-round-robin
```

Syntax: [no] ipx gns-round-robin

Possible values: N/A

Default value: N/A

ipx netbios-allow

Enables NetBIOS broadcasts (type 20) to be routed over IPX. IPX must be enabled on the router and a network number and frame type defined for each IPX interface.

EXAMPLE:

```
HP9300(config)# ipx netbios-allow
```

Syntax: ipx netbios-allow

Possible values: N/A

Default value: disabled

ipx rip-filter

Defines IPX/RIP filters for the router. IPX must be enabled on the router for this command to be operational.

EXAMPLE:

```
HP9300(config)# ipx rip-filter 2 permit 11005000 fffff00
```

or

```
HP9300(config)# ipx rip-filter 2 permit any any
```

Syntax: ipx rip-filter <index> permit | deny <network-number> | any <network-mask> | any

Possible values: up to 32 RIP filters can be defined for a router

Default value: N/A

ipx rip-filter-group

Allows a group of filters to be applied globally to all IPX interfaces at the Global Level, or individually to an IPX interface at the Interface Level. The filter can be applied to either incoming or outgoing traffic.

EXAMPLE:

To apply previously defined filters 1, 2, 3, and 10 to all incoming IPX RIP routes across all interfaces, enter the following command:

```
HP9300(config)# ipx rip-filter-group in 1 2 3 10
```

To apply filters on an individual interface (e.g. interface 4/11) basis versus globally, enter the following:

```
HP9300(config)# int e 4/11
```

```
HP9300(config-if-4/11)# ipx rip-filter-group in 1 2 3 10
```

Syntax: ipx rip-filter-group in | out <index>

Possible values: in | out, filter I ds

Default value: disabled

ipx sap-access-list

Configures access lists for filtering Service Advertisement Protocol (SAP) replies sent on a routing switch's IPX interfaces. You configure IPX SAP access lists on a global basis, then apply them to the IPX inbound or outbound filter group on specific interfaces. You can configure up to 32 access lists. The same access list can be applied to multiple interfaces.

EXAMPLE:

```
HP9300(config-ipx-router)# ipx sap-access-list 10 deny efef.1234.1234.1234
```

Syntax: [no] ipx sap-access-list <num> deny | permit <network>[.<node>] [<network-mask>.<node-mask>] [<service-type>[<server-name>]]

Possible values: The <num> parameter specifies the access list number and can be from 1 – 32.

The **deny | permit** parameter specifies whether the routing switch allows the SAP update or denies it.

The <network>[.<node>] parameter specifies the IPX network. Optionally, you also can specify a specific node (host) on the network. The <network> parameter can be an eight-digit hexadecimal number from 1 – FFFFFFFE. To specify all networks ("any"), enter –1 as the network number. If the network number has leading zeros, you do not need to specify them. For example, you can specify network 0000abab as "abab".

The node is a 48-bit value represented by three four-digit numbers joined by periods; for example, 1234.1234.1234.

The [<network-mask>.<node-mask>] parameter lets you specify a comparison mask for the network and node. The mask consists of zeros (0) and ones (f). Ones indicate significant bits. For example, to configure a mask that matches on network abcdef*xx*, where *xx* can be any value and the node address can be any value, specify the following mask: ffffff00.0000.0000.0000

The **in | out** parameter of the **ipx sap-filter-group** command specifies whether the ACLs apply to incoming traffic or outgoing traffic.

Default value: N/A

ipx sap-filter

Defines IPX/SAP filters for all IPX interfaces on the router. The IPX network number and frame type must be defined for the interfaces for this command to be operational.

EXAMPLE:

```
HP9300(config)# ipx sap-filter 5 permit any server1
```

or

```
HP9300(config)# ipx sap-filter 5 permit 0004 any
```

Syntax: ipx sap-filter <index> permit | deny <server-type> | any <server-name> | any

Possible values: Filter IDs

Default value: Disabled

ipx sap-filter-group

Allows a group of defined IPX/SAP filters to be applied either globally (at the Global Level) or individually (at the Interface Level) to IPX interfaces on the router.

The filter can be applied to either incoming or outgoing traffic.

EXAMPLE:

To apply previously defined filters 2, 3, and 10 to all incoming IPX SAP server traffic across all interfaces, enter the following command:

```
HP9300(config)# ipx sap-filter-group in 2 3 5
```

To apply filters on an individual interface basis instead of a global basis (for example, apply a filter to interface 4/11), enter the following:

```
HP9300(config)# int 4/11
```

```
HP9300(config-if)# ipx sap-filter-group in 2 3 5
```

Syntax: ipx sap-filter-group in | out <index>

Possible values: in or out, defined filter indexes

Default value: N/A

lock-address ethernet

Allows you to limit the number of devices that have access to a specific port. The parameter **address-count** will allow only that value of learned addresses to have access to the port. Access violations will be reported in SNMP traps.

EXAMPLE:

```
HP9300(config)# lock-address eth 4/11 addr 15
```

Syntax: lock-address ethernet <portnum> [addr-count <num>]

Possible values: Address count: 1 – 2,048

Default value: Address count: 8

logging

You can save SNMP traps locally to an event log on the switch or router by turning this feature on. You also can configure the device to use one or two third-party SyslogD servers and modify the message level and facility using this command. In addition, you can change the number of log messages the local Syslog buffer will retain.

EXAMPLE:

To enable logging of SNMP traps to a locally saved event log, enter the following:

```
HP9300(config)# logging on
```

Syntax: logging on | off

Possible values: on, off

Default value: on (enabled)

EXAMPLE:

To specify two third-party SyslogD servers to receive Syslog messages in addition to the device's local Syslog buffer, enter commands such as the following:

```
HP9300(config)# logging 10.0.0.99
HP9300(config)# logging 209.157.23.69
```

Syntax: logging <ip-addr> | <server-name>

NOTE: If you specify two SyslogD servers, the HP device uses the same facility and message level for messages to both servers.

Possible values: N/A

Default value: N/A

EXAMPLE:

To change the logging facility from the default facility user to local7, enter the following command:

```
HP9300(config)# logging local7
```

Syntax: logging facility <facility-name>

Possible values:

- kern – kernel messages
- user – random user-level messages
- mail – mail system
- daemon – system daemons
- auth – security/authorization messages
- syslog – messages generated internally by syslogd
- lpr – line printer subsystem
- news – netnews subsystem
- uucp – uucp subsystem
- sys9 – cron/at subsystem
- sys10 – reserved for system use
- sys11 – reserved for system use
- sys12 – reserved for system use
- sys13 – reserved for system use
- sys14 – reserved for system use
- cron – cron/at subsystem
- local0 – reserved for local use
- local1 – reserved for local use
- local2 – reserved for local use
- local3 – reserved for local use
- local4 – reserved for local use

- local5 – reserved for local use
- local6 – reserved for local use
- local7 – reserved for local use

Default value: user

EXAMPLE:

To disable logging of debugging and informational messages, enter the following commands:

```
HP9300(config)# no logging buffered debugging
HP9300(config)# no logging buffered informational
```

Syntax: [no] logging buffered <level>

Possible values: The <level> can be emergencies, alerts, critical, errors, warnings, notifications, informational, or debugging.

Default value: All message levels are enabled by default. You can disable message levels individually.

EXAMPLE:

To change the local buffer capacity from the default 50 to 100, enter the following commands:

```
HP9300(config)# logging buffered 100
HP9300(config)# end
HP9300# reload
```

Syntax: logging buffered <num-entries>

Possible values: <num-entries> can be 50 – 100

Default value: default local buffer capacity is 50 entries.

EXAMPLE:

By default, a message is logged whenever a user logs into or out of the CLI's User EXEC or Privileged EXEC mode. If you want to disable logging of users' CLI access, enter the following command:

```
HP9300(config)# no logging enable user-login
```

Syntax: [no] logging enable user-login

Possible values: N/A

Default value: User logins are logged by default.

m2 active-management

In Chassis devices containing redundant management modules, changes the default assignment of the active management module. By default, the redundant management module in the lower slot number becomes the active redundant management module. You must use this command to override the default and make the redundant management module in the higher slot number the default active module.

NOTE: This command applies only to devices containing redundant management modules.

NOTE: The change does not take effect until you reload the system. If you save the change to the active module's system-config file before reloading, the change persists across system reloads. Otherwise, the change affects only the next system reload.

EXAMPLE:

To override the default and specify the active redundant management module, enter a command such as the following:

```
HP9300(config)# m2 active-management 5
```

Syntax: m2 active-management <slot-num>

- Slots on the HP 9304M are numbered 1 – 4, from top to bottom.
- Slots on the HP 9308M are numbered 1 – 8, from left to right.

This command overrides the default and makes the redundant management module in slot 5 the active module following the next reload. The change affects only the next reload and does not remain in effect for future reloads.

To make the change permanent across future reloads, enter the write memory command to save the change to the system-config file, as shown in the following example:

```
HP9300(config)# m2 active-management 5
HP9300(config)# write mem
```

Possible values: a valid Chassis device slot number

Default value: the redundant management module in the lower-numbered Chassis device slot is the default active module

m2 load-standby-source

Copies the system software image file onto the flash memory of a standby redundant management module. Use this command if your primary boot source is TFTP.

During switchover, the standby redundant management module boots using the system software it copied from the other redundant management module's primary or secondary flash. By default, the standby module uses the same flash (primary or secondary) as the active module uses for its primary boot source.

However, a standby redundant management module does not boot from a TFTP or BootP server. If the active module uses a TFTP or BootP server as the primary boot source, you must copy the flash code (system software) onto the active module's flash, then instruct the active module to boot the standby module using the software.

NOTE: This command applies only to devices containing redundant management modules.

EXAMPLE:

To copy the routing switch flash code for software version 05.2.00 (HPR05200) from a TFTP server to the active redundant management module's primary flash, then load the standby module using the copied flash code, enter the following commands:

```
HP9300# copy tftp flash 209.157.22.5 HPR05200.bin primary
HP9300# m2 load-standby-source primary
```

Syntax: copy tftp flash <tftp-ip-addr> <filename> primary | secondary

Syntax: m2 load-standby-source primary | secondary

Possible values: see above

Default value: N/A

m2 sync boot-standby

Configures a device containing redundant management modules to automatically update the boot flash on the standby redundant management module to the version installed on the active redundant management module. The "active" module is the redundant management module that is active when you enter the command or select the Web management option.

By default, the active redundant management module does not synchronize its boot flash code with the boot flash code on the standby redundant management module. Thus, it is possible for the redundant management modules to have different boot flash releases. If the active module is updated with boot code that contains a problem, the system can still run using the standby module, which is running the older boot code.

NOTE: This command applies only to devices containing redundant management modules.

EXAMPLE:

To enable boot code synchronization:

```
HP9300(config)# m2 sync boot-standby
```

Syntax: m2 sync boot-standby

Possible values: N/A

Default value: N/A

m2 sync running-config

Changes the interval at which the active redundant management module updates the running-config file on the standby redundant management module. You also can disable the updates.

At system startup and each time you save the system-config file, the active redundant management module updates the system-config file on the standby redundant management module. By default, the active redundant management module also sends a copy of the running-config file to the standby redundant management module every 10 seconds. Thus, if a switchover occurs, the standby module contains not only the configuration information in the system-config file, but also the unsaved configuration changes, which are contained in the running-config file.

NOTE: This command applies only to devices containing redundant management modules.

EXAMPLE:

To change the synchronization interval for the running-config file to 15 seconds, enter the following commands:

```
HP9300(config)# m2 sync running-config 15
```

Syntax: m2 sync running-config [<num>]

You can specify from 4 – 20 seconds. If you set the interval to 0, the file is not copied to the standby redundant management module. If you do not specify a value, the current value is shown. Here is an example:

```
HP9300(config)# m2 sync running-config

Current m2 sync running-config-standby period is 15 seconds
```

Possible values: 0 or 4 – 20 seconds; 0 disables synchronization of the running-config file.

Default value: 10 seconds

mac-age-time

Sets the aging period for all address entries in the switch or router address table.

EXAMPLE:

```
HP9300(config)# mac-age 600
```

Syntax: mac-age-time <value>

Possible values: 0 – 65,535 seconds. If you specify 0, the entries do not age.

Default value: 300 seconds

mac filter

Allows you to filter on MAC addresses.

NOTE: You cannot use Layer 2 filters to filter Layer 4 information. To filter Layer 4 information, use IP access policies or ACLs. See the “Configuring IP and IP/RIP” and “Using Access Control Lists (ACLs)” chapters in the *Advanced Configuration and Management Guide*.

EXAMPLE:

```
HP9300(config)# mac filter 2 deny 3565.3475.3676 any etype eq 806
```

Syntax: mac filter <filter-num> permit | deny any | <H.H.H> any | <H.H.H> etype | IIc | snap eq | gt | lt | neq <frame-type>

Possible values:

The <filter-num> is 1 – 64 (64 is the default system-max setting). If you use the **system-max mac-filter-sys** command, you can increase the maximum number of MAC filters support to 128 for global filter definitions.

The **permit | deny** argument determines the action the software takes when a match occurs.

The first **any** | <H.H.H> argument specifies the source MAC address matching criteria. Use the keyword **any** to apply the filter to all source MAC addresses. If you use **any**, you do not need the mask keyword. Enter the MAC address as three groups of two bytes each separated by a period. Example: 0260.8C00.0102. The mask is bit-significant; if the mask has a bit set to one, then the corresponding bit in the MAC address is significant (that is, it is checked).

The second **any** | <H.H.H> argument specifies the destination MAC address matching criteria. Use the keyword **any** to apply the filter to all destination MAC addresses. If you use **any**, you do not need the mask keyword. Enter the MAC address as three groups of two bytes each separated by a period. Example: 0260.8C00.0102. The mask is bit-significant; if the mask has a bit set to one, then the corresponding bit in the MAC address is significant (that is, it is checked).

Use the **etype | llc | snap** argument if you want to filter on information beyond the source and destination address. The MAC filter allows for you to filter on the following encapsulation types:

- **etype** (Ethertype) – a two byte field indicating the protocol type of the frame. This can range from 0x0600 to 0xFFFF.
- **llc** (IEEE 802.3 LLC1 SSAP and DSAP) – a two byte sequence providing similar function as the EtherType but for an IEEE 802.3 frame.
- **snap** (IEEE 802.3 LLC1 SNAP) – a specific LLC1 type packet.

To determine which type of frame is used on your network, use a protocol analyzer. If byte 12 of an Ethernet packet is equal to or greater than 0600 (hex), it is an Ethernet framed packet. Any number below this indicates an IEEE 802.3 frame (byte 12 will now indicate the length of the data field). Some well-known Ethernet types are 0800 (TCP/IP), 0600 (XNS), and 8137 (Novell Netware). Refer to RFC 1042 for a complete listing of EtherTypes.

For IEEE 802.3 frame, you can further distinguish the SSAP and DSAP of LLC header. Some well-known SAPs include: FE (OSI), F0 (NetBIOS), 42 (Spanning Tree BPDU), and AA (SNAP). Usually the DSAP and SSAP are the same.

NOTE: You must type in both bytes, otherwise the software will fill the field, left justified with a 00. Refer to RFC 1042 for a complete listing of SAP numbers.

SNAP is defined as an IEEE 802.3 frame with the SSAP, DSAP, and control field set to AA, AA, and 03. Immediately following these is a five-byte SNAP header. The first three bytes in this header are not used by the MAC filters. However, the next two bytes usually are set to the EtherType, so you can define the EtherType inside the SNAP header that you want to filter on.

The **eq | gt | lt | neq** argument specifies the possible operator: eq (equal), gt (greater than), lt (less than) and neq (not equal).

The <frame-type> argument is a hexadecimal number for the frame type. For example, the hex number for ARP is 806.

Default value: N/A

Additional Examples of Layer 2 MAC Filter Definitions

```
HP9300(config)# mac filter 1 permit any any etype eq 0800
```

This filter configures the device to permit (forward) any inbound packet with the Ethertype field set to 0800 (IP).

```
HP9300(config)# mac filter 2 deny 0080.0020.000 ffff.ffff.0000 any etype eq 0800
```

This filter configures the device to deny an inbound packet with the first four bytes set to 0800.0020.xxxx *and* an EtherType field set to 0800 (IP). The destination field does not matter.

```
HP9300(config)# mac filter 3 deny any 00e0.5200.1234 ffff.ffff.ffff snap eq 0800
```

This filter configures the device to deny any inbound IEEE 802.3 packet with a destination set to 00e0.5200.1234 and a SNAP EtherType set to 0800. The source address does not matter.

```
HP9300(config)# mac filter 32 permit any any
```

This filter permits all packets. This filter is used as the last filter assigned in a filter-group that has previous deny filters in the group.

Abbreviating the Address or Mask

Address and Mask abbreviations are allowed. However, be careful when configuring them. The default fill character is a 0 and it will fill a byte range as left-justified. This applies only to the MAC address and mask. A range of frame types cannot be filtered. Each frame type must be entered. Here are some examples.

```
HP9300(config)# mac filter 1 deny 0800.0700 ffff.ff00 any
```

This command expands to the following: `mac filter 1 deny 0800.0700.0000 ffff.ff00.0000`

The filter shown above denied forwarding of an inbound frame that has the source address set to 080007 as the first three bytes. All other information is not significant.

Here is another example of the fill feature.

```
HP9300(config)# mac filter 2 deny 0260.8C00.0102 0.0.ffff any
```

This command expands to the following: `mac filter 1 deny 0260.8C00.0102 0000.0000.ffff any`

Since the fill character is 0's and the fill is left justified, certain filters will not allow for abbreviations. For example, suppose you want to deny an inbound packet that contained a broadcast destination address. Enter the following command:

```
HP9300(config)# mac filter 5 deny any ff ff
```

This command contains a destination of address all F's and mask of F's. The command expands to the following:

```
HP9300(config)# mac filter 1 deny any 00ff.0000.0000 00ff.0000.0000
```

Here is another example for DSAP and SSAP.

```
HP9300(config)# mac filter 10 deny any any llc eq F0
```

This command expands to the following: `mac filter 2 deny any any llc eq 00f0`

If you want to filter on both the SSAP and DSAP, then the following example shows this:

```
HP9300(config)# mac filter 4 deny any 0020.0010.1000 ffff.ffff.0000 llc eq e0e0
```

mac filter log_en

Enables logging of packets that are denied by Layer 2 MAC filters. When you enable this feature, the device generates Syslog entries and SNMP traps for denied packets.

See "show logging" on page 20-35 for information about log entries generated by this feature.

EXAMPLE:

```
HP9300(config)# mac filter log_en
```

Syntax: mac filter log_en

Possible values: N/A

Default value: Disabled

mirror-port ethernet

Enables and assigns a specific port to operate as a mirror port for other ports on a switch or router. Once enabled, you can connect an external traffic analyzer to the port for traffic analysis.

You also need to enable the **monitor** command on a port for it to be mirrored by this port.

EXAMPLE:

To assign port 1 on module 1 as the mirror port and port 5 on the same module as the port to be monitored, enter the following:

```
HP9300(config)# mirror-port e 1/1
HP9300(config)# interface e 1/5
HP9300(config-if-1/5)# monitor both
```

NOTE: To define a mirror port on a Chassis device, define a slot number in addition to the port number as seen in the syntax below.

Syntax: mirror-port ethernet <portnum>

Possible values: N/A

Default value: Undefined

module

Adds a hardware module to an HP Chassis device.

EXAMPLE:

To add an 8-port Gigabit Ethernet management module to slot 3 in a Chassis device, enter the following command:

```
HP9300(config)# module 3 8-port-gig-management-module
```

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

The <slot-num> parameter indicates the Chassis device slot number.

- Slots on the HP 9304M are numbered 1 – 4, from top to bottom.
- Slots on the HP 9308M are numbered 1 – 8, from left to right.

See the “Hardware OverView” chapter of the *Installation and Getting Started Guide* for more information about slot and port numbering.

The <module-type> parameter can be one of the following.

Table 6.2: Module Options

Module Type	Part Number and Description	Module String
Redundant Management modules	J4845A HP ProCurve 9300 GigLX Redundant Management Module (8-port)	8-port-gig-management-module
	J4846A HP ProCurve 9300 GigSX Redundant Management Module (8-port)	8-port-gig-management-module
	J4847A J4847A HP ProCurve 9300 Redundant Management Module (0-port)	0-port-management-module

Table 6.2: Module Options (Continued)

Module Type	Part Number and Description	Module String
Management modules	J4141A ProCurve 9300 10/100 Management Module (16-port)	16-port-copper-management-module
	J4144A HP ProCurve 9300 Gigabit SX Management Module (8-port)	8-port-gig-management-module
	J4146A HP ProCurve 9300 Gigabit 4LX/ 4SX Management Module (8-port)	8-port-gig-management-module
Unmanaged modules	J4842A ProCurve Gigabit Copper Management Module (8-port)	8-port-gig-copper-module
	J4140A HP ProCurve 9300 10/100 Module (24-port)	24-port-copper-module
	J4142A HP ProCurve 9300 100Base FX Module (24-port MT-RJ)	24-port-100fx-module
	J4143A HP ProCurve 9300 Gigabit SX Module (8-port)	8-port-gig-module
	J4145A HP ProCurve 9300 Gigabit 4LX/ 4SX Module (8-port)	8-port-gig-module
	J4844A HP ProCurve 9300 GigLX Module (8-port)	8-port-gig-module

Possible values: see above

Default value: N/A

multicast filter

Configures a Layer 2 filter for multicast packets. You can filter on all multicast packets or on specific multicast groups.

EXAMPLE:

To configure a Layer 2 multicast filter to filter all multicast groups, then apply the filter to ports 2/4, 2/5, and 2/8, enter the following commands:

```
HP9300(config)# multicast filter 1 any
HP9300(config-mcast-filter-id-1)# exclude-ports ethernet 2/4 to 2/5 ethernet 2/8
HP9300(config-mcast-filter-id-1)# write mem
```

EXAMPLE:

To configure a multicast filter to block all multicast traffic destined for multicast addresses 0100.5e00.5200 – 0100.5e00.52ff on port 4/8, enter the following commands:

```
HP9300(config)# multicast filter 2 any 0100.5e00.5200 ffff.ffff.ff00
HP9300(config-mcast-filter-id-2)# exclude-ports ethernet 4/8
HP9300(config-mcast-filter-id-2)# write mem
```

The software calculates the range by combining the mask with the multicast address. In this example, all but the last two bits in the mask are “significant bits” (ones). The last two bits are zeros and thus match on any value.

Syntax: [no] multicast filter <filter-ID> any | ip udp mac <multicast-address> | any [mask <mask>] [vlan <vlan-id>]

The parameter values are the same as the for the broadcast filter command. In addition, the multicast filter command requires the **mac** <multicast-address> **| any** parameter, which specifies the multicast address. Enter **mac any** to filter on all multicast addresses. Enter **mac** followed by a specific multicast address to filter only on that multicast address.

To filter on a range of multicast addresses, use the **mask** <mask> parameter. For example, to filter on multicast groups 0100.5e00.5200 – 0100.5e00.52ff, use **mask ffff.ffff.ff00**. The default mask matches all bits (is all Fs). You can leave the mask off if you want the filter to match on all bits in the multicast address.

Possible values: see above

Default value: N/A

multicast limit

Specifies the maximum number of multicast packets the device can forward each second. By default the device sends multicasts and all other traffic at wire speed and is limited only by the capacities of the hardware. However, if other devices in the network cannot handle unlimited multicast traffic, this command allows you to relieve those devices by throttling the multicasts at the HP device.

NOTE: The multicast limit does not affect broadcast or unicast traffic. However, you can use the **broadcast limit** and **unknown-unicast limit** commands to control these types of traffic. See “broadcast limit” on page 6-11 and “unknown-unicast limit” on page 6-65.

EXAMPLE:

```
HP9300(config)# multicast limit 30000
```

Syntax: multicast limit <num>

Possible values: 0 – 4294967295

Default value: N/A

no

Disables other commands. To disable a command, place the word ***no*** before the command.

password-change

Allows you to define those access points from which the system password can be defined. Options are **cli**, **console-cli**, **telnet-cli**, or **any**. The **any** option allows the password to be modified from a serial port, Telnet session, at any level of the user interface.

EXAMPLE:

To allow password changes from a serial port console connection only, enter the following command:

```
HP9300(config)# password-change console-cli
```

Syntax: password-change cli | console-cli | telnet-cli | any

Possible values: cli, console-cli, telnet-cli, or any

Default value: None

perf-mode

Allows you to define the performance mode as 'high' to allow flow control to activate at an earlier stage, when heavy congestion exists on the network. This feature must be saved to memory and the system reset before it becomes active.

EXAMPLE:

```
HP9300(config)# perf-mode hi
```

Syntax: perf-mode normal | hi

Possible values: hi

Default value: normal

ping

Verifies connectivity to an HP switch or routing switch or other device. The command performs an ICMP echo test to confirm connectivity to the specified device.

NOTE: If you address the ping to the IP broadcast address, the device lists the lists the first four responses to the ping.

EXAMPLE:

```
HP9300#(config) ping 192.22.2.33
```

Syntax: ping <ip-addr> | <hostname> [count <num>] [timeout <msec>] [ttl <num>] [size <byte>] [no-fragment] [quiet] [verify] [data <1 – 4 byte hex>]

The only required parameter is the IP address or host name of the device.

NOTE: If the device is an HP switch or routing switch, you can use the host name only if you have already enabled the Domain Name Server (DNS) resolver feature on the device from which you are sending the ping. See the "Configuring Basic Features" chapter of the *Installation and Getting Started Guide*.

The **count** <num> parameter specifies how many ping packets the device sends. You can specify from 1 – 4294967296. The default is 1.

The **timeout** <msec> parameter specifies how many milliseconds the HP device waits for a reply from the pinged device. You can specify a timeout from 1 – 4294967296 milliseconds. The default is 5000 (5 seconds).

The **ttl** <num> parameter specifies the maximum number of hops. You can specify a TTL from 1 – 255. The default is 64.

The **size** <byte> parameter specifies the size of the ICMP data portion of the packet. This is the payload and does not include the header. You can specify from 0 – 4000. The default is 16.

The **no-fragment** parameter turns on the "don't fragment" bit in the IP header of the ping packet. This option is disabled by default.

The **quiet** parameter hides informational messages such as a summary of the ping parameters sent to the device and instead only displays messages indicating the success or failure of the ping. This option is disabled by default.

The **verify** parameter verifies that the data in the echo packet (the reply packet) is the same as the data in the echo request (the ping). By default the device does not verify the data.

The **data** <1 – 4 byte hex> parameter lets you specify a specific data pattern for the payload instead of the default data pattern, "abcd", in the packet's data payload. The pattern repeats itself throughout the ICMP message (payload) portion of the packet.

NOTE: For numeric parameter values, the CLI does not check that the value you enter is within the allowed range. Instead, if you do exceed the range for a numeric value, the software rounds the value to the nearest valid value.

Possible values: see above

Default value: see above

privilege

Augments the default access privileges for an access level. When you configure a user account, you can give the account one of three privilege levels: full access, port-configuration access, and read-only access. Each privilege level provides access to specific areas of the CLI by default:

- Full access provides access to all commands and displays.
- Port-configuration access gives access to:
  - The User EXEC and Privileged EXEC levels, and the port-specific parts of the CONFIG level
  - All interface configuration levels
- Read-only access gives access to:
  - The User EXEC and Privileged EXEC levels

EXAMPLE:

To enhance the port-configuration privilege level so users also can enter **ip** commands at the global CONFIG level (useful for adding IP addresses for multinetting), enter the following command:

```
HP9300(config)# privilege configure level 4 ip
```

In this command, configure specifies that the enhanced access is for a command at the global CONFIG level of the CLI. The level 4 parameter indicates that the enhanced access is for privilege level 4 (port-configuration). All users with port-configuration privileges will have the enhanced access. The **ip** parameter indicates that the enhanced access is for the IP commands. Users who log in with valid port-configuration level user names and passwords can enter commands that begin with "ip" at the global CONFIG level.

Syntax: [no] privilege <cli-level> level <privilege-level> <command-string>

The <cli-level> parameter specifies the CLI level and can be one of the following values:

- **exec** – EXEC level; for example, HP9300> or HP9300#
- **configure** – CONFIG level; for example, HP9300(config)#
- **interface** – interface level; for example, HP9300(config-if-6)#
- **virtual-interface** – virtual-interface level; for example, HP9300(config-vif-6)#
- **rip-router** – RIP router level; for example, HP9300(config-rip-router)#
- **ospf-router** – OSPF router level; for example, HP9300(config-ospf-router)#
- **dvmrp-router** – DVMRP router level; for example, HP9300(config-dvmrp-router)#
- **pim-router** – PIM router level; for example, HP9300(config-pim-router)#
- **bgp-router** – BGP4 router level; for example, HP9300(config-bgp-router)#
- **port-vlan** – Port-based VLAN level; for example, HP9300(config-vlan)#
- **protocol-vlan** – Protocol-based VLAN level

The <privilege-level> indicates the privilege level you are augmenting.

The **level** parameter specifies the privilege-level. You can specify one of the following:

- **0** – Full access (super-user)
- **4** – Port-configuration access
- **5** – Read-only access

The <command-string> parameter specifies the command you are allowing users with the specified privilege level to enter. To display a list of the commands at a CLI level, enter "?" at that level's command prompt and press Return.

qos mechanism

Configures the queuing method used for QoS. Two queuing methods are available:

- Weighted (the default) – A weighted fair queuing algorithm is used to rotate service among the four queues. The rotation is based on the weights you assign to each queue. This is the default queuing method and uses a default set of queue weights. This method rotates service among the four queues, forwarding a specific number of packets in one queue before moving on to the next one.

  The number of packets serviced during each visit to a queue depends on the percentages you configure for the queues. The software automatically converts the percentages you specify into weights for the queues.
- Strict – The software assigns the maximum weights to each queue, to cause the queuing mechanism to serve as many packets in one queue as possible before moving to a lower queue. This method biases the queuing mechanism to favor the higher queues over the lower queues. For example, strict queuing processes as many packets as possible in qosp3 before processing any packets in qosp2, then processes as many packets as possible in qosp2 before processing any packets in qosp1, and so on.

EXAMPLE:

To change the queuing method from weighted fair queuing to strict queuing:

```
HP9300(config)# qos mechanism strict
```

Syntax: [no] qos mechanism strict | weighted

Possible values: See above.

Default value: weighted

qos name

Changes the QoS queue names from their defaults. The default queue names are qosp3, qosp2, qosp1, and qosp0.

EXAMPLE:

To rename queue qosp3 (the premium queue) to "92-octane":

```
HP9300(config)# qos name qosp3 92-octane
HP9300(config)# write mem
```

Syntax: qos name <old-name> <new-name>

Possible values: The <old-name> parameter specifies the name of the queue before the change.

The <new-name> parameter specifies the new name of the queue. You can specify an alphanumeric string up to 32 characters long.

qos profile

Changes the minimum guaranteed bandwidth percentages of the queues. If you change the percentages for the queues, the software changes the weights, which changes the number of visits a queue receives during a full queue cycle and also the number of packets sent from each queue during each visit. For example, if you change the percentages so that queue qosp3 receives a weight of 5, then the system processes five packets in that queue during each visit to the queue.

NOTE: The weighted fair queuing method is based on packet-level scheduling. As a result, a queue's bandwidth percentage does not necessarily reflect the exact bandwidth share the queue receives. This is due to the effects of variable size packets.

EXAMPLE:

To change the minimum guaranteed bandwidth percentages of the queues:

```
HP9300(config)# qos profile qosp3 75 qosp2 10 qosp1 10 qosp0 5
Profile qosp3     : PREMIUM     bandwidth requested  75% calculated  75%
Profile qosp2     : HIGH        bandwidth requested  10% calculated  13%
Profile qosp1     : NORMAL      bandwidth requested  10% calculated   8%
Profile qosp0     : BEST-EFFORT bandwidth requested   5% calculated   4%
HP9300(config)# write mem
```

Notice that the CLI displays the percentages you request and the percentages the device can provide based on your request. The values are not always the same, as explained below.

Syntax: [no] qos profile <queue> <percentage> <queue> <percentage> <queue> <percentage> <queue> <percentage>

Each <queue> parameter specifies the name of a queue. You can specify the queues in any order on the command line, but you must specify each queue.

The <percentage> parameter specifies a number for the percentage of the device's outbound bandwidth that are allocating to the queue.

NOTE: The percentages you enter must equal 100. Also, the percentage for the premium queue (the highest priority queue) must be at least 50.

If you enter percentages that are less than the minimum percentages supported for a queue, the CLI recalculates the percentages to fall within the supported minimums. Here is an example. In this example, the values entered for all but the best-effort queue (the lowest priority queue) are much lower than the minimum values supported for those queues.

Possible values: See above.

Default value: The following table lists the default minimum guaranteed bandwidth percentages of the queues:

Queue	Default Minimum Percentage of Bandwidth
qosp3	80%
qosp2	15%
qosp1	3.3%
qosp0	1.7%

qos tagged-priority

Allows you to reassign 802.1p priorities to different QoS queues. Tagged priority applies to tagged packets that come in from tagged ports. These packets have a tag in the header that specifies the packet's VLAN ID and its 802.1p priority tag value, which is 3 bits long.

You can specify how the HP device interprets the 3-bit priority information by reassigning the priority levels to other queues. For example, if you want the device to disregard the 802.1p priority and instead assign the priority based on other items (VLAN, port, and so on), you can configure the device to set all the 802.1p priorities to the best-effort queue (qosp0). If a tagged packet's 802.1p priority level is always in the qosp0 queue, then the packet's outbound queue is affected by other items such as incoming port, VLAN, and so on.

EXAMPLE:

To reassign all 802.1p priority levels 2 – 7 to the best-effort queue (qosp0), enter the following commands:

```
HP9300(config)# qos tagged-priority 2 qosp0
HP9300(config)# qos tagged-priority 3 qosp0
HP9300(config)# qos tagged-priority 4 qosp0
```

```
HP9300(config)# qos tagged-priority 5 qosp0
HP9300(config)# qos tagged-priority 6 qosp0
HP9300(config)# qos tagged-priority 7 qosp0
HP9300(config)# write mem
```

Syntax: [no] qos tagged-priority <num> <queue>

The <num> parameter can be from 0 – 7 and specifies the IEEE 802.1 equivalent to one of the four QoS queues.

The <queue> parameter specifies the queue to which you are reassigning the priority level. You must specify one of the named queues. The default names are qosp3, qosp2, qosp1, and qosp0. The example above reassigns the 802.1p levels to queue qosp0. (There is no need to reassign levels 0 and 1 in this case, because they are already assigned to qosp0 by default.)

Possible values: See above.

Default value: By default, an HP device interprets the prioritization information in the 3-bit priority tag as follows:

Priority Level	Queue
6, 7	qosp3
4, 5	qosp2
2, 3	qosp1
0, 1	qosp0

quit

Returns you from any level of the CLI to the User EXEC mode.

EXAMPLE:

```
HP9300(config)# quit
HP9300>
```

Syntax: quit

Possible values: N/A

Default value: N/A

radius-server

Identifies a RADIUS server and sets other RADIUS authentication parameters for authenticating access to the HP device.

EXAMPLE:

HP9300(config)# radius-server host 209.157.22.99

Syntax: radius-server host <ip-addr> | <server-name> [auth-port <number>] [acct-port <number>]

<ip-addr> | <server-name> is either an IP address or an ASCII text string.

<auth-port> is the Authentication port number; it is an optional parameter. The default is 1645.

<acct-port> is the Accounting port number; it is an optional parameter. The default is 1646.

Syntax: radius-server [key <key-string>] [timeout <number>] [retransmit <number>] [dead-time <number>]

The key <key-string> parameter is the encryption key; valid key string length is from 1 – 16.

The **timeout** <number> is how many seconds to wait before declaring a RADIUS server timeout for the authentication request. The default timeout is 3 seconds. The range of possible timeout values is from 1 – 15.

The **retransmit** <number> is the maximum number of retransmission attempts. When an authentication request timeout, the HP software will retransmit the request up to the maximum number of retransmissions configured. The default retransmit value is 3 seconds. The possible retransmit value is from 1 – 5.

The **dead-time** parameter is not used in this software release. When the software allows multiple authentication servers, this parameter will specify how long the HP device waits for the primary authentication server to reply before deciding the server is dead and trying to authenticate using the next server. The dead-time value can be from 1 – 5 seconds. The default is 3.

Possible values: see above

Default value: see above

rarp

Enters a static IP RARP entry for static routes on an HP router.

EXAMPLE:

```
HP9300(config)# rarp 1 1245.7654.2348 192.53.4.2

HP9300(config)# exit

HP9300# write mem
```

Syntax: rarp <num> <mac-addr>.<ip-addr> ethernet <portnum>

Possible values: Up to 16 static RARP entries can be assigned

Default value: N/A

relative-utilization

Allows you to configure uplink utilization lists that display the percentage of a given uplink port's bandwidth that is used by a specific list of downlink ports. The percentages are based on 30-second intervals of RMON packet statistics for the ports. Both transmit and receive traffic is counted in each percentage.

NOTE: This feature is intended for ISP or collocation environments in which downlink ports are dedicated to various customers' traffic and are isolated from one another. If traffic regularly passes between the downlink ports, the information displayed by the utilization lists does not provide a clear depiction of traffic exchanged by the downlink ports and the uplink port.

Each uplink utilization list consists of the following:

- Utilization list number (1, 2, 3, or 4)
- One or more uplink ports
- One or more downlink ports

Each list displays the uplink port and the percentage of that port's bandwidth that was utilized by the downlink ports over the most recent 30-second interval. You can configure up to four bandwidth utilization lists.

EXAMPLE:

To configure a link utilization list with port 1/1 as the uplink port and ports 1/2 and 1/3 as the downlink ports.

```
HP9300(config)# relative-utilization 1 uplink eth 1/1 downlink eth 1/2 to 1/3
```

Syntax: [no] relative-utilization <num> uplink ethernet <portnum> [to <portnum> | <portnum>…]
downlink ethernet <portnum> [to <portnum> | <portnum>…]

Possible values: The <num> parameter specifies the list number. You can configure up to four lists. Specify a number from 1 – 4.

The **uplink ethernet** parameters and the port number(s) you specify after the parameters indicate the uplink port(s).

The **downlink ethernet** parameters and the port number(s) you specify after the parameters indicate the downlink port(s).

Default value: N/A

rmon alarm

Defines what MIB objects are monitored, the type of thresholds that will be monitored (falling, rising or both), the value of those thresholds, and the sample type (absolute or delta).

An alarm event will be reported each time that a threshold is exceeded. The alarm entry also defines the action (event) to take should the threshold be exceeded.

A sample CLI alarm entry and its syntax is shown below:

EXAMPLE:

```
HP9300(config)# rmon alarm 1 ifInOctets.6 10 delta rising-threshold 100 1 falling
threshold 50 1 owner nyc02
```

Syntax: rmon alarm <entry-number> <MIB-object.interface-number> <sampling-time> <sample-type> <threshold-type> <threshold-value> <event-number> <threshold-type> <threshold-value> <event-number> owner <text>

`Possible values:`

- Threshold type: rising-threshold or falling threshold
- Sample type: delta or absolute

Default value: N/A

rmon event

There are two elements to the RMON event group 9, the event control table and the event log table.

The event control table defines the action to be taken when an alarm is reported. Defined events can be displayed by entering the CLI command, **show event**.

The event log table collects and stores reported events for retrieval by an RMON application.

EXAMPLE:

```
HP9300(config)# rmon event 1 description ‘testing a longer string’ log-and-trap
public owner nyc02
```

Syntax: rmon event <event-entry> description <text-string> log | trap | log-and-trap owner <rmon-station>

Possible values: N/A

Default value: N/A

rmon history

All active HP switch and router ports by default will generate two RMON history (group 2) control data entries. If a port becomes inactive, then the two entries will automatically be deleted.

Two history entries are generated for each switch by default:

- a sampling of statistics every 30 seconds
- a sampling of statistics every 30 minutes

You can modify how many of these historical entries are saved in an event log (buckets) as well as how often these intervals are taken. The station (owner) that collects these entries can also be defined.

To review the control data entry for each port or interface, enter the **show rmon history** command.

EXAMPLE:

```
HP9300(config)# rmon history 1 interface 1 buckets 10 interval 10 owner nyc02
```

Syntax: rmon history <entry-number> interface <portnum> buckets <number> interval <sampling-interval> owner <text-string>

Possible values: Buckets: 1 – 50 entries.

Default value: N/A

route-map

Creates a route map and places you in the Route Map CONFIG level of the CLI. A route map is a named set of match conditions and parameter settings that the router can use to modify route attributes and to control redistribution of the routes into other protocols. See the “Configuring BGP4” chapter of the *Advanced Configuration and Management Guide*.

EXAMPLE:

To add instance 1 of a route map named "GET_ONE" with a permit action, enter the following command.

```
HP9300(config)# route-map GET_ONE permit 1
HP9300(config-bgp-routemap GET_ONE)#
```

Syntax: route-map <map-name> permit | deny <num>

As shown in this example, the command prompt changes to the Route Map level. You can enter the match and set statements at this level. See “Route Map Commands” on page 15-1. Also see the “Configuring BGP4” chapter of the *Advanced Configuration and Management Guide*.

The <map-name> is a string of characters that names the map. Map names can be up to 32 characters in length. You can define up 50 route maps on the router.

The **permit | deny** parameter specifies the action the router will take if a route matches a match statement.

- If you specify **deny**, the routing switch does not advertise or learn the route.
- If you specify **permit**, the routing switch applies the match and set statements associated with this route map instance.

The <num> parameter specifies the instance of the route map you are defining. Each route map can have up to 50 instances. Routes are compared to the instances in ascending numerical order. For example, a route is compared to instance 1, then instance 2, and so on.

Possible values: N/A

Default value: N/A

route-only

Globally disables Layer 2 switching on an HP routing switch.

NOTE: Make sure you really want to disable all Layer 2 switching operations before you use this option. Consult your reseller or HP for information.

NOTE: As an alternative to disabling switching globally, you can disable it on individual interfaces. See “route-only” on page 7-24.

EXAMPLE:

```
HP9300(config)# route-only
HP9300(config)# exit
HP9300# write mem
HP9300# reload
```

Syntax: [no] route-only

Possible values: N/A

Default value: Enabled

router appletalk

This is a launch command that allows you to move to the AppleTalk configuration level of the Command Line Interface (CLI).

This command is not supported on HP switches.

EXAMPLE:

```
HP9300(config)# router appletalk
HP9300(config-atalk-router)# end
HP9300# write mem
HP9300# end
HP9300# reload
```

NOTE: You must reset the system when AppleTalk is first enabled on the router using the **router appletalk** command. If you have previously reset the system and defined AppleTalk interface(s), and the interface configuration represents an addition, then no reset of the system is required.

Syntax: router appletalk

Possible values: N/A

Default value: disabled

router bgp

This is a launch command that allows you to move to the BGP configuration level.

This command is not supported on HP switches.

EXAMPLE:

```
HP9300(config)# router bgp
HP9300(config-bgp-router)#
```

Syntax: router bgp

Possible values: N/A

Default value: disabled

router dvmrp

This is a launch command that allows you to move to the DVMRP configuration level.

This command is not supported on HP switches.

NOTE: You must reload the software after enabling this protocol to place the change into effect.

EXAMPLE:

```
HP9300(config)# router dvmrp
HP9300(config-dvmrp-router)# end
HP9300(config)# reload
```

Syntax: router dvmrp

Possible values: N/A

Default value: disabled

router ipx

Activates IPX routing on a router.

This command is not supported on HP switches.

NOTE: You must reload the software after enabling this protocol to place the change into effect.

EXAMPLE:

```
HP9300(config)# router ipx
HP9300(config-ipx-router)# end
HP9300(config)# reload
```

Syntax: router ipx

Possible values: N/A

Default value: disabled

router ospf

Activates OSPF routing on an HP router and launches you into the OSPF configuration level.

This command is not supported on HP switches.

EXAMPLE:

```
HP9300(config)# router ospf
HP9300(config-ospf-router)#
```

Syntax: router ospf

Possible values: N/A

Default value: disabled

router pim

Activates PIM multicast on a router.

This command is not supported on HP switches.

NOTE: You must reload the software after enabling this protocol to place the change into effect.

EXAMPLE:

```
HP9300(config)# router pim
HP9300(config-pim-router)# end
HP9300(config)# reload
```

Syntax: router pim

Possible values: N/A

Default value: disabled

router rip

Activates RIP routing on a router and launches you into that configuration level to assign or modify RIP parameters.

This command is not supported on HP switches.

NOTE: You must reload the software after enabling this protocol to place the change into effect.

EXAMPLE:

```
HP9300(config)# router rip
HP9300(config-rip-router)# end
HP9300(config)# reload
```

Syntax: router rip

Possible values: N/A

Default value: disabled

router srp

This is a launch command that enables the SRP feature. SRP allows redundant paths to be assigned. Parameters for SRP are set using the Interface level command **ip srp address** <ip-addr>…

This command is not supported on HP switches.

NOTE: You must reload the software after enabling this protocol to place the change into effect.

To enable SRP on the router, enter the following:

```
HP9300(config)# router srp
HP9300(config-srp-router)# end
HP9300(config)# reload
```

Possible values: N/A

Default value: disabled

router vrrp

Launches you into the VRRP configuration level.

This command is not supported on HP switches.

EXAMPLE:

```
HP9300(config)# router vrrp
HP9300(config-vrrp-router)#
```

Syntax: router vrrp

Possible values: N/A

Default value: disabled

server port

Adds a profile for an application TCP or UDP port. This command applies only when you are using a routing switch for the Globally-distributed Server Load Balancing (SLB) feature. See the “Route Health Injection” chapter of the *Advanced Configuration and Management Guide*. When you add a profile for an application port, the health check for the port is automatically enabled.

Example: To add a profile for TCP port 80 and thus enable its health check, enter the following commands:

```
HP9300(config)# server port 80
HP9300(config-port-80)#
```

Syntax: server port <num>

See for “Application Port Commands” on page 19-1 for information about the commands you can enter at the Application Port level.

Possible values: TCP port number

Default value: N/A

server real-name

Identifies a Web server for Globally-distributed Server Load Balancing (SLB). Globally-distributed SLB allows the same web site (and same IP address) to reside on multiple servers, which usually are in geographically dispersed locations. See the "Route Health Injection" chapter of the *Advanced Configuration and Management Guide*.

Use the **server real-name** command to identify the web sites for which the HP routing switch is helping to provide geographically-distributed SLB.

EXAMPLE:

```
HP9300(config)# server real S2 209.157.22.249

HP9300(config-rs-S2)# port http keepalive
```

Syntax: [no] server real-name <name> <vip>

The <name> parameter identifies the third-party SLB or real server. This value does not need to match a value on the third-party SLB or real server. The value simply identifies the third-party SLB or real server uniquely on the routing switch.

The <vip> parameter is the IP address of the web site. If the web server is directly attached to the routing switch, this is the IP address of the IP address on the web server. If the web server is attached to a third-party SLB, the VIP is the virtual IP address configured on the third-party SLB for the web site.

Possible values: see above

Default value: N/A

service password-encryption

Enables password encryption. When encryption is enabled, users cannot learn the device's passwords by viewing the configuration file. Password encryption is enabled by default.

NOTE: Password encryption does not encrypt the password in Telnet packets sent to the device. This feature applies only to the configuration file.

EXAMPLE:

```
HP9300(config)# no service password-encryption
```

Syntax: [no] service password-encryption

Possible values: N/A

Default value: Enabled

show

Displays a variety of configuration and statistical information about the switch or router. See "Show Commands" on page 20-1.

snmp-client

Restricts SNMP management access to the HP device to the host whose IP address you specify. No other device except the one with the specified IP address can access the HP device through an SNMP application.

If you want to restrict access from Telnet or the Web, use one or two of the following commands:

- **telnet-client** – restricts Telnet access. See "telnet-client" on page 6-63.
- **web-client** – restricts Web access. See "web-client" on page 6-66.

If you want to restrict all management access, you can use the commands above and the **snmp-client** command or you can use the following command: **all-client**. See "all-client" on page 6-7.

EXAMPLE:

To restrict SNMP access to the HP device to the host with IP address 209.157.22.26, enter the following command:

```
HP9300(config)# snmp-client 209.157.22.26
```

Syntax: [no] snmp-client <ip-addr>

Possible values: a valid IP address. You can enter one IP address with the command. You can use the command up to ten times for up to ten IP addresses.

Default value: N/A

snmp-server community

Assigns an SNMP community string for the system:

- read-only (public)
- read-write (private)

EXAMPLE:

```
HP9300(config)# snmp-server community planet1 ro
```

Syntax: snmp-server community [0 | 1] <string> ro | rw

The **0 | 1** parameter specifies whether you want the software to encrypt the string (**1**) or show the string in the clear (**0**). The default is **1**.

The <string> parameter specifies the community string name.

The **ro | rw** parameter specifies whether the string is read-only (**ro**) or read-write (**rw**).

Possible values: Up to 32 alphanumeric characters for the community string.

Default value: The default read-only (**ro**) community string is “public”. HP devices do not have a default read-write (**rw**) community string.

snmp-server contact

Identifies a system contact. You can designate a contact name for the switch or router and save it in the configuration file for later reference. You can later access contact information using the **show snmp server** command.

EXAMPLE:

```
HP9300(config)# snmp-server contact N Y Ngo
```

Syntax: snmp-server contact <text>

Possible values: up to 32 alphanumeric characters for the system contact text string

Default value: N/A

snmp-server enable traps

When the command is preceded with **no**, the command is used to stop certain traps from being generated by a system. The following SNMP traps are collected by default:

- authentication key
- cold-start
- link-up
- link-down
- new-root
- topology-change

- power-supply-failure
- locked-address-violation

To stop reporting incidences of links that are down, enter the following commands:

```
HP9300(config)# no snmp-server enable traps link-down
```

Syntax: [no] snmp-server enable traps <trap-type>

Possible values: trap type (for example, cold-start, new-root, and so on)

Default value: All of the following SNMP traps are enabled and will be generated by default for a system:

- authentication key
- cold-start
- link-up
- link-down
- new-root
- topology-change
- power-supply-failure
- locked-address-violation

To disable a fan failure trap or power supply trap, use one of the following values:

- ps1
- ps2
- ps3
- ps4
- fan1
- fan2
- fan3
- fan4

snmp-server host

Assigns or removes a station as an SNMP trap receiver. To assign the trap receiver, use the command **snmp-server host**. To later remove the trap receiver feature, enter **no snmp-server host**.

EXAMPLE:

To disable a station as an SNMP trap receiver, enter the following:

```
HP9300(config)# no snmp-server host 192.22.3.33 public
```

Syntax: snmp-server host <ip-addr> [0 | 1] <string>

The <ip-addr> parameter specifies the IP address of the trap receiver.

The **0 | 1** parameter specifies whether you want the software to encrypt the string (**1**) or show the string in the clear (**0**). The default is **1**.

The <string> parameter specifies an SNMP community string configured on the HP device. The string can be a read-only string or a read-write string. The string is not used to authenticate access to the trap host but is instead a useful method for filtering traps on the host. For example, if you configure each of your HP devices that use the trap host to send a different community string, you can easily distinguish among the traps from different HP devices based on the community strings.

Possible values: IP address of trap receiver station, community string

Default value: no system default

snmp-server location

Identifies a system location for the switch or router. This information is saved in the configuration file for later reference. You can later access system location information using the **show snmp server** command.

EXAMPLE:

```
HP9300(config)# snmp-server location oakcabldg519
```

Syntax: snmp-server location <text>

Possible values: up to 32 alphanumeric characters for the snmp-server location text string

Default value: N/A

snmp-server pw-check

Disables password checking for SNMP set requests. If a third-party SNMP management application does not add a password to the password field when it sends SNMP set requests to an HP device, by default the HP device rejects the request. You can disable this password checking with the **no snmp-server pw-check** command.

EXAMPLE:

```
HP9300(config)# no snmp-server pw-check
```

Syntax: [no] snmp-server pw-check

Possible values: N/A

Default value: N/A

snmp-server trap-source

Specifies a port or virtual interface whose first configured IP address the HP device must use as the source for all SNMP traps sent by the device.

EXAMPLE:

```
HP9300(config)# snmp trap-source ethernet 4/11
```

Syntax: snmp trap-source ethernet <portnum> | ve <num>

Possible values: The **ethernet** <portnum> parameter specifies a physical port on the device. Alternatively, you can specify a virtual interface using the **ve** <num> parameter, where <num> is the number of a virtual interface configured on the device.

Default value: N/A

sntp poll-interval

This parameter sets how often clock updates are requested from an SNTP server.

EXAMPLE:

To configure the switch or router to poll for clock updates from an SNTP server every 15 minutes, enter the following:

```
HP9300(config)# sntp poll-interval 900
```

Syntax: sntp poll-interval <1 – 65535>

Possible values: 1 – 65535 seconds

Default value: 1800 seconds

sntp server

Allows you to define the SNTP server that will be used for clock synchronization for the HP switch or router. You can enter the SNTP server's IP address or its host name.

Up to three SNTP server entries can be defined.

EXAMPLE:

To define the SNTP server (IP address 208.99.8.95) that will be polled by the switch or router for time updates, enter:

```
HP9300(config)# sntp server
```

Syntax: sntp server <ip-addr> | <hostname> <version>

The <version> parameter specifies the SNTP version the server is running and can be from 1 – 4. The default is 1. You can configure up to three SNTP servers by entering three separate **sntp server** commands.

Possible values:

Default value: No system default

spanning-tree

Enables or disables (no) Spanning Tree on the switch or router. This change can be viewed by the **show spanning tree** command.

- For switches, this feature is enabled by default.
- For routers, this feature is disabled by default.

To disable this feature, enter **no spanning-tree**. To later re-enable spanning tree on the router, enter **spanning-tree**.

EXAMPLE:

To disable spanning tree, enter the following:

```
HP9300(config)# no span
HP9300(config)# end
HP9300(config)# write memory
```

EXAMPLE:

To enable spanning tree, enter the following:

```
HP9300(config)# spanning-tree
```

Syntax: [no] spanning-tree

Possible values: N/A

Default value: Enabled on switches. Disabled on routing switches.

spanning-tree <parameter>

Spanning Tree bridge and port parameters are configurable using one CLI command. When no port-based VLANs are active on the system, spanning tree parameters are set at the Global CONFIG Level.

When port-based VLANs are active on the system, spanning tree protocol bridge and port parameters can be configured globally at the VLAN Level. Additionally, you can disable or enable STP on an interface basis.

NOTE: If VLANs are active on a switch or router, spanning-tree will not be seen as an option at the Global CONFIG Level of the CLI but will be an option of the VLAN Level.

All bridge and port parameters have default values and do not need to be modified unless required to match network needs. Additionally, all values will be globally applied to the switch or router. By default this feature is enabled on switches and disabled on routers.

You can modify the following STP Parameters:

1. Modify bridge parameters—forward delay, maximum age, hello time, and priority
2. Modify port parameters—priority and path cost

EXAMPLE:

Suppose you want to enable spanning tree on a system in which no port-based VLANs are active and change the hello-time from the default value of 2 to 8 seconds. Additionally, suppose you want to change the path and priority costs for port 5 only. To do so, enter the following commands.

```
HP9300(config)# span hello-time 8
HP9300(config)# span ethernet 5 path-cost 15 priority 64
```

Here is the syntax for global STP parameters.

Syntax: spanning-tree [forward-delay <value>] | [hello-time <value>] | [maximum-age <time>] | [priority <value>]

Here is the syntax for port STP parameters.

Syntax: spanning-tree ethernet <portnum> path-cost <value> | priority <value>

Possible values: see below

Bridge Parameters:

- Forward-delay: Possible values: 4 – 30 seconds. Default is 15 seconds.
- Max-age: Possible values: 6 – 40 seconds. Default is 20 seconds.
- Hello-time: Possible values: 1 – 10 seconds. Default is 2 seconds.
- Priority: Possible values: 1 – 65,535. Default is 32,678.

Port Parameters:

- Path: Possible values: 1-65,535. Default: Auto

NOTE: The default value 'Auto' means that the port will adjust the default value automatically based on the port speed. The default value is based on the following:

- Half-duplex ports: 1000/port speed
- Full-duplex ports: (1000/port speed)/2

- Priority: possible values are 0 – 255. Default is 128.

spanning-tree single <parameter>

Configures single spanning tree. Single spanning tree enables you to configure a single instance of the Spanning Tree Protocol (STP) to run on all the port-based VLANs on a device.

Single-instance STP uses the same parameters, with the same value ranges and defaults, as the default STP on HP devices (multiple-instance STP), which is described in the previous section.

static-mac-address

Defines a static MAC address on an individual switch or switching port to ensure it is not aged out.

The options **router-type** and **host-type** are not available for the HP 6308M-SX and HP 6208M-SX.

EXAMPLE:

```
HP9300(config)# static 1145.5563.67FF e12 7 router-type
```

Syntax: static-mac-address <mac-addr> ethernet <portnum> [priority <0-7>] [host-type | router-type]

Possible values: The priority can be 0 – 7 (0 is lowest and 7 is highest).

Default value: host-type; 0 priority

system-max

Allows you to modify the default settings for parameters that use system memory. The configurable parameters and their defaults and maximums differ depending on the device. To display the configurable parameters, their

defaults, and the maximum configurable values for each, enter the following command at any level of the CLI: **show default values**. See “show default” on page 20-6.

EXAMPLE:

To increase the system capacity of an HP 9304M or HP 9308M for IP routes from the default 10000 to 50000, enter the following command:

```
HP9300(config)# system-max ip-route 50000
```

Syntax: system-max <parameter> <value>

Possible values: These depend on the device you are configuring. See the System Parameters section in the **show default values** display. The CLI will display the acceptable range if you enter a value that is outside the range.

tacacs-server

Identifies a TACACS or TACACS+ server and sets other TACACS/TACACS+ parameters for authenticating access to the HP device.

EXAMPLE:

HP9300(config)# tacacs-server host 209.157.22.99

Syntax: tacacs-server host <ip-addr> | <server-name> [auth-port <number>]

The only required parameter is the IP address or host name of the server.

NOTE: To specify the server's host name instead of its IP address, you must first identify a DNS server using the **ip dns server-address** <ip-addr> command at the global CONFIG level. See the “Configuring Basic Features” chapter of the *Installation and Getting Started Guide*.

The **auth-port** parameter specifies the UDP port number of the authentication port on the server. The default port number is 49.

Syntax: tacacs-server [key <key-string>] [timeout <number>] [retransmit <number>] [dead-time <number>]

The **key** parameter specifies the value that the HP device sends to the server when trying to authenticate user access. The TACACS/TACACS+ server uses the key to determine whether the HP device has authority to request authentication from the server. The key can be from 1 – 16 characters in length.

The **timeout** parameter specifies how many seconds the HP device waits for a response from the TACACS/TACACS+ server before either retrying the authentication request or determining that the TACACS/TACACS+ server is unavailable and moving on to the next authentication method in the authentication-method list. The timeout can be from 1 – 15 seconds. The default is 3 seconds.

The **retransmit** parameter specifies how many times the HP device will resend an authentication request when the TACACS/TACACS+ server does not respond. The retransmit value can be from 1 – 5 times. The default is 3 times.

The **dead-time** parameter is not used in this software release. When the software allows multiple authentication servers, this parameter will specify how long the HP device waits for the primary authentication server to reply before deciding the server is dead and trying to authenticate using the next server. The dead-time value can be from 1 – 5 seconds. The default is 3.

Possible values: see above

Default value: see above

tag-type

This parameter defines the value that will be sent out on a packet to indicate it is part of a tagged VLAN port. The 802.1q standard recognizes the value of 8100 for this purpose. Other values can be assigned to this parameter but are not recommended.

EXAMPLE:

```
HP9300(config)# tag-type 8100
```

Syntax: tag-type <value>

Possible values: 1 – 65535

Default value: 8100

telnet-client

Restricts Telnet management access to the HP device to the host whose IP address you specify. No other device except the one with the specified IP address can access the HP device's CLI through Telnet.

If you want to restrict access from SNMP or the Web, use one or two of the following commands:

- **snmp-client** – restricts SNMP access. See "snmp-client" on page 6-56.
- **web-client** – restricts web access. See "web-client" on page 6-66.

If you want to restrict all management access, you can use the commands above and the **telnet-client** command or you can use the following command: **all-client**. See "all-client" on page 6-7.

EXAMPLE:

To restrict Telnet access to the HP device to the host with IP address 209.157.22.26, enter the following command:

```
HP9300(config)# telnet-client 209.157.22.26
```

Syntax: [no] telnet-client <ip-addr>

Possible values: a valid IP address. You can enter one IP address with the command. You can use the command up to ten times for up to ten IP addresses.

Default value: N/A

telnet-server

Enables or disables Telnet access to an HP switch or router. By default, Telnet access is allowed on a system.

EXAMPLE: To disable Telnet access to a switch, enter the following:

```
HP9300(config)# no telnet-server
```

Syntax: [no] telnet-server

Possible values: Enabled or disabled

Default value: Enabled

telnet-timeout

Defines how many minutes a Telnet session can remain idle before it is timed out. An idle Telnet session is a session that is still sending TCP ACKs in response to keepalive messages from the HP device, but is not being used to send data.

By default, the Telnet timeout is zero (which means Telnet sessions do not time out).

NOTE: HP devices also have another, non-configurable Telnet timer used to close sessions that have ended abnormally. This mechanism is enabled regardless of the setting of the Telnet timeout. The HP device sends TCP keepalive messages to the Telnet client once a minute. If the client fails to respond to two consecutive keepalive messages, the HP device concludes that the TCP session has ended abnormally and immediately ends the session. A typical cause of a session ending abnormally is the client rebooting during the TCP session.

EXAMPLE:

```
HP9300(config)# telnet-timeout 120
```

Syntax: telnet-timeout <0 – 240>

Possible values: 0 – 240 minutes

Default value: 0 minutes (no timeout)

trunk

Allows you to add a trunk group and connect the ports in the group to a switch, router, or server for high-speed connections. See the "Configuring Basic Features" chapter of the *Installation and Getting Started Guide* for more trunk configuration rules and other information.

NOTE: The ports in a trunk group make a single logical link. Therefore, all the ports in a trunk group must be connected to the same device at the other end.

NOTE: On Chassis device with Gigabit Ethernet modules, you can configure a trunk group that spans two Gigabit Ethernet modules and contains up to eight ports.

EXAMPLE:

To assign ports 1, 2, and 3 to a trunk group on the HP 6208M-SX, enter the following command:

```
HP6208(config)# trunk switch e 1 to 3
```

A trunk group must then also be configured on the connecting switch or routing at the other end of the trunk group. The **switch** parameter in the above command can refer to another HP switch or routing switch.

If you are going to connect to a server, then enter the following command:

```
HP6208(config)# trunk server e1 to 3
```

This will connect a trunk group of ports 1, 2, and 3 to a server.

Syntax: trunk [server | switch] ethernet <primary-portnum> to <portnum>

The **server | switch** parameter specifies whether the trunk ports will be connected to a server or to another switch or routing switch. This parameter affects the type of load balancing performed by the device. See the "Configuring Basic Features" chapter of the *Installation and Getting Started Guide*. The default is **switch**.

Each **ethernet** parameter introduces a port group.

The <primary-portnum> **to** <portnum> parameters specify the ports. The first port must be a primary port and the remaining ports must be the ports that follow it. The primary port is always the lowest number in the following port ranges:

- HP 9304M and HP 9308M: 1 – 4, 5 – 8, 9 – 12, 13 – 16 and 17 – 18 and 21 –24
- HP 6208M-SX and HP 6308M-SX: 1 – 4 and 5 – 8 or 1 – 2, 3 – 4, 5 – 6, 7 – 8

EXAMPLE:

To configure a trunk group consisting of two groups of ports, 1/1 – 1/4 on module 1 and 4/5 – 5/8 on module 4, enter the following commands:

```
HP9300(config)# trunk ethernet 1/1 to 1/4 ethernet 4/5 to 4/8

HP9300(config)# write mem

HP9300(config)# exit

HP9300# reload
```

Syntax: trunk [server | switch] ethernet <primary-portnum> to <portnum> ethernet <primary-portnum> to <portnum>

The **server | switch** parameter specifies whether the trunk ports will be connected to a server or to another switch or routing switch. This parameter affects the type of load balancing performed by the HP device. See the "Configuring Basic Features" chapter of the *Installation and Getting Started Guide*. The default is **switch**.

Each **ethernet** parameter introduces a port group.

The <primary-portnum> **to** <portnum> parameters specify a port group. Notice that each port group must begin with a primary port. After you enter this command, the primary port of the first port group specified (which must be

the group with the lower port numbers) becomes the primary port for the entire trunk group. For Gigabit Ethernet modules, the primary ports are 1, 3, 5, and 7.

Possible values: see above

Default value: N/A

unknown-unicast limit

Specifies the maximum number of unknown-unicast packets the device can forward each second. By default the device sends unknown unicasts and all other traffic at wire speed and is limited only by the capacities of the hardware. However, if other devices in the network cannot handle unlimited unknown-unicast traffic, this command allows you to relieve those devices by throttling the unknown unicasts at the HP device.

NOTE: The unknown-unicast limit does not affect broadcast or multicast traffic. However, you can use the **broadcast limit** and **multicast limit** commands to control these types of traffic. See “broadcast limit” on page 6-11 and “multicast limit” on page 6-44.

EXAMPLE:

```
HP9300(config)# unknown-unicast limit 30000
```

Syntax: unknown-unicast limit <num>

Possible values: 0 – 4294967295

Default value: N/A

username

Configures a local user account. For each user account, you specify the user name. You also can specify the following parameters:

- A password
- The privilege level, which can be one of the following:
- Full access (super-user). This is the default.
- Port-configuration access
- Read-only access

EXAMPLE:

To configure a user account, enter a command such as the following at the global CONFIG level of the CLI.

```
HP9300(config)# username wonka password willy
```

This command adds a user account for a super-user with the user name "wonka" and the password "willy", with privilege level super-user. This user has full access to all configuration and display features.

NOTE: If you configure user accounts, you must add a user account for super-user access before you can add accounts for other access levels. You will need the super-user account to make further administrative changes.

```
HP9300(config)# username waldo privilege 5 password whereis
```

This command adds a user account for user name "waldo", password "whereis", with privilege level read-only. Waldo can look for information but cannot make configuration changes.

Syntax: [no] username <user-string> privilege <privilege-level> password | nopassword <password-string>

The privilege parameter specifies the privilege-level. You can specify one of the following:

- **0** – Full access (super-user)
- **4** – Port-configuration access
- **5** – Read-only access

The default privilege level is **0**. If you want to assign full access to the user account, you can enter the command without "**privilege 0**", as shown in the command example above.

The **password | nopassword** parameter indicates whether the user must enter a password. If you specify **password**, enter the string for the user's password.

NOTE: You must be logged on with super-user access (privilege level 0, or with a valid Enable password for super-user access) to add user accounts or configure other access parameters.

vlan

Creates or changes the CLI focus to a port-based VLAN.

EXAMPLE:

```
HP9300(config)# vlan 200 by port
HP9300(config)# vlan 200 name Prod Marketing
```

Syntax: vlan <num> by port

Syntax: vlan <num> name <string>

NOTE: The second command is optional and also creates the VLAN if the VLAN does not already exist. You can enter the first command after you enter the second command if you first exit to the global CONFIG level of the CLI.

Possible values: VLAN ID 1 – 1024; VLAN name can be a string up to 16 characters. You can use blank spaces in the name if you enclose the name in double quotes (for example, "`Prod Marketing`".)

Default value: N/A

vlan max-vlans

Allows you to assign a set number of VLANs to be supported on a switch or router. This allows you to set a smaller value than the default to preserve memory on the system.

EXAMPLE:

```
HP9300(config)# vlan max-vlans 200
```

Syntax: vlan max-vlans <value>

Possible values: 1 – 1,024

Default value: 32

web-client

Restricts Web management access to the HP device to the host whose IP address you specify. No other device except the one with the specified IP address can access the HP device's Web management interface.

If you want to restrict access from SNMP or Telnet, use one or two of the following commands:

- **snmp-client** – restricts SNMP access. See "snmp-client" on page 6-56.
- **telnet-client** – restricts Telnet access to the CLI. See "telnet-client" on page 6-63.

If you want to restrict all management access, you can use the commands above and the **web-client** command or you can use the following command: **all-client**. See "all-client" on page 6-7.

EXAMPLE:

To restrict Web access to the HP device to the host with IP address 209.157.22.26, enter the following command:

```
HP9300(config)# web-client 209.157.22.26
```

Syntax: [no] web-client <ip-addr>

Possible values: a valid IP address. You can enter one IP address with the command. You can use the command up to ten times for up to ten IP addresses.

Default value: N/A

web-management

Sets configuration options on the Web management interface. By default the Web management interface is enabled.

EXAMPLE:

To disable the Web management interface on a switch or router, enter the following:

```
HP9300(config)# no web-management
```

Syntax: [no] web-management [allow-no-password | enable | front-panel | list-menu]

Possible values: The **allow-no-password option** disables password authentication for the Web management interface

The **enable** option enables the Web management interface on the switch or router.

The **front-panel** option causes the front panel frame, which contains a graphic depicting the switch or router, to be displayed on the Web management interface.

The **list-menu** option causes the List (pre-06.x) menu to be displayed on the Web management interface, instead of the Tree menu.

Default value: Password authentication and the front panel are enabled by default. The List menu is disabled by default. (This means the Tree menu is enabled by default.)

write memory

Saves the running configuration into the startup-config file.

EXAMPLE:

```
HP9300(config)# wr mem
```

Syntax: write memory

Possible values: N/A

Default value: N/A

write terminal

Displays the running configuration of the HP switch or router on the terminal screen.

NOTE: This command is equivalent to the **show running-config** command.

EXAMPLE:

```
HP9300(config)# wr term
```

Syntax: write terminal

Possible values: N/A

Default value: N/A